PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-039795
(43)Date of publication of application : 12.02.1999

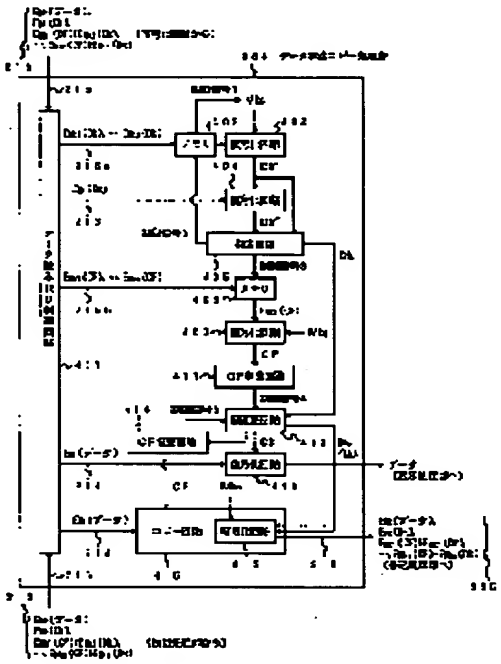
(51)Int.CI. G11B 20/10
G06F 12/14
G09C 1/00
H04L 9/16
H04L 9/36

(21)Application number : 09-186837
(22)Date of filing : 11.07.1997

(71)Applicant : TOSHIBA CORP
(72)Inventor : KATO TAKEHISA

(54) DEVICE FOR PREVENTING UNAUTHORIZED DATA COPY AND METHOD THEREFOR AND RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To surely protect an attack of an unauthorized person against a part under copy management in data. SOLUTION: In this device to be used for equipment for copying digital data, the digital data 215 has an enciphered data itself EDk and enciphered copy management information (EMk1(CF)+EMk1(Dk),..., EMkn (CF)+EMkn(Dk)) for managing approval of copying this data itself EDk. When the digital data is judged to be disapproval of its copy, provided contents of this copy management information are satisfied with prescribed conditions (411), the digital data is not copied at all (412).



LEGAL STATUS

[Date of request for examination] 18.09.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－39795

(43)公開日　平成11年(1999)２月12日

(51)Int.Cl.[6]	識別記号	ＦＩ		
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｅ	
			３２０Ｂ	
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	
Ｈ０４Ｌ　9/16		Ｈ０４Ｌ　9/00	６４３	

審査請求　未請求　請求項の数10　ＯＬ　（全 22 頁）　最終頁に続く

(21)出願番号　特願平9－186837

(22)出願日　平成９年(1997)７月11日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　加藤　岳久
東京都府中市東芝町１番地　株式会社東芝府中工場内

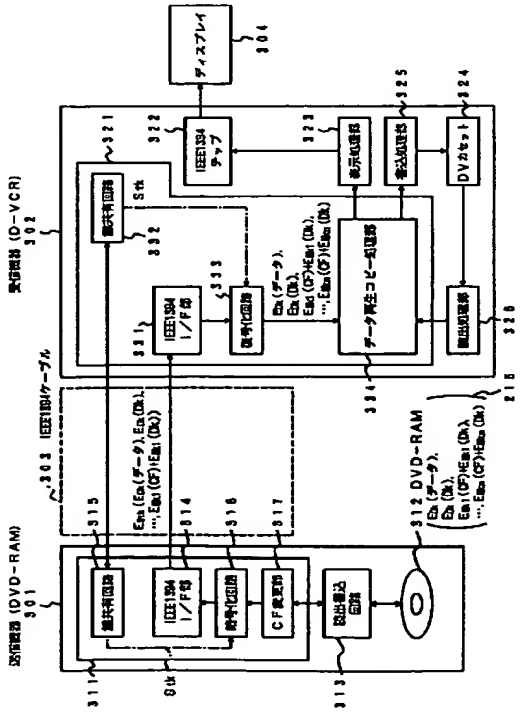
(74)代理人　弁理士　鈴江　武彦　（外６名）

(54)【発明の名称】　不正データコピー防止装置及び方法並びに記録媒体

(57)【要約】

【課題】　データ内のコピー管理を行う部分に対する不正者の攻撃を確実に防御できる。

【解決手段】　デジタルデータをコピーする機器に用いられる不正データコピー防止装置において、デジタルデータ２１５は、暗号化されたデータ本体２１４と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報２１２と有し、コピー管理情報の内容が所定の条件を満たして、デジタルデータがコピー不許可と判定されたとき（４１１）には、デジタルデータのコピーを行わない（４１２）不正データコピー防止装置。



【特許請求の範囲】
【請求項１】　デジタルデータをコピーする機器に用いられる不正データコピー防止装置において、
前記デジタルデータは、
暗号化されたデータ本体と、
当該データ本体のコピー許可について管理する暗号化されたコピー管理情報とを有し、
前記コピー管理情報の内容が所定の条件を満たして、前記デジタルデータがコピー不許可と判定されたときには、前記デジタルデータのコピーを行わないことを特徴とする不正データコピー防止装置。
【請求項２】　デジタルデータをコピーする機器に用いられる不正データコピー防止装置において、
前記デジタルデータは、
暗号化されたデータ本体と、
当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、
前記データ本体を復号するための鍵情報とを有し、
前記コピー管理情報の内容が所定の条件を満たして、前記デジタルデータがコピー不許可と判定されたときには、前記デジタルデータ内の前記鍵情報を変更する鍵変更手段を備えたことを特徴とする不正データコピー防止装置。
【請求項３】　前記コピー管理情報は、
前記デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報と、当該デジタルデータを何回コピーしたかを示すコピー回数管理情報からなり、
前記世代管理情報が所定の世代数となり、前記コピー回数管理情報が所定のコピー回数となると、コピー不許可であることを示す請求項１又は２記載の不正データコピー防止装置。
【請求項４】　前記コピー管理情報は、
前記デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報を有し、当該世代管理情報が所定の世代数となるとコピー不許可であることを示すものであり、
かつ、その情報ビット数を３ビット以上として、最初のデータのコピーのコピー以上の世代のデータまでコピー許可管理可能としたことを特徴とする請求項１又は２記載の不正データコピー防止装置。
【請求項５】　前記デジタルデータを送信機器と受信機器間で伝送する場合であり、かつ前記送信機器又は前記受信機器に適用される不正データコピー防止装置であって、
前記送信機器と前記受信機器と間で共有された一時鍵を暗号鍵もしくは復号鍵として、両者間で伝送される前記デジタルデータを暗号化もしくは復号化する暗号化手段もしくは復号化手段を備えたことを特徴とする請求項１乃至４のうち何れか１項記載の不正データコピー防止装置。
【請求項６】　デジタルデータをコピーする機器に用いられる不正データコピー防止方法において、
前記デジタルデータは、
暗号化されたデータ本体と、
当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、
前記データ本体を復号するための鍵情報とを有し、
前記コピー管理情報の内容が所定の条件を満たして、前記デジタルデータがコピー不許可と判定されたときには、前記デジタルデータ内の前記鍵情報を変更することを特徴とする不正データコピー防止方法。
【請求項７】　デジタルデータをコピーする機器に用いられる不正データコピー防止方法において、
前記デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報と、当該デジタルデータを何回コピーしたかを示すコピー回数管理情報からなるコピー管理情報を前記デジタルデータに付加し、
前記世代管理情報が所定の世代数となり、前記コピー回数管理情報が所定のコピー回数となると、コピー不許可として不正なデータコピーを防止することを特徴とする不正データコピー防止方法。
【請求項８】　暗号化されたデータ本体と、
当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、
前記データ本体を復号するための鍵情報と、
前記コピー管理情報を復号するための鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体。
【請求項９】　暗号化されたデータ本体と、
前記データ本体を復号するためのデータ暗号鍵が当該データ暗号鍵を暗号鍵として暗号化されてなる第１の鍵情報と、
前記データ暗号鍵が複数の暗号鍵によりそれぞれ暗号化されてなる複数の第２の鍵情報と、
前記データ本体のコピー許可について管理するコピー管理情報が、前記複数の暗号鍵によりそれぞれ暗号化されてなる複数の第３の鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体。
【請求項１０】　暗号化されたデータ本体と、
前記データ本体を復号するためのデータ暗号鍵が当該データ暗号鍵を暗号鍵として暗号化されてなる第１の鍵情報と、
前記データ暗号鍵が複数の暗号鍵によりそれぞれ暗号化されてなる複数の第２の鍵情報と、
前記データ本体のコピー許可について管理するコピー管理情報が、前記データ暗号鍵を暗号鍵として暗号化されてなる第３の鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】この発明はデータコピー防止装置及び方法並びに記録媒体、特にデジタル化された文書、音声、画像、プログラム等のデータを不正にコピーすることを防止する不正データコピー防止装置及び方法並びに記録媒体に関するものである。

【０００２】

【従来の技術】近年、デジタル記録再生機器の開発、製品化が進み、これらのデジタル記録再生機器間で画質や音質の劣化なくデータをコピーすることが可能となっている。しかし高画質な複製は、海賊版と呼ばれる不正なコピーを増加させ、著作権が侵害されるという問題がある。このような不正なコピーは確実に防止されなければならない。というのも、Ｄ－ＶＣＲやＤＶＤ－ＲＡＭ等の大容量デジタル記録再生機器の出現により、デジタル化された著作物は簡単にコピーされ、不特定多数への配布が可能となり、これによりデジタル画像等の著作権者に危機感を与えているからである。

【０００３】不正コピーを行う手段としては種々の方法が考えられるが、とにかく不正者はＤＶＤ－ＲＯＭドライブやＤ－ＶＣＲといった再生装置等の機器からコピー対象とするデータを受け取り、ＤＶＤ－ＲＡＭ等の他のデジタル記録機器で複写するという手続きを踏む必要がある。

【０００４】従来のＤＶＤ等ほど大容量でないデジタル記録再生機器、例えばＤＡＴやＭＤでは、その不正なデータコピーを防止する手段として、ＳＣＭＳ（シリアルコピーマネージメントシステム）を用いている。

【０００５】ＳＣＭＳでは、例えばＣＤからＭＤ（又はＤＡＴ）へ、もしくはＭＤ（又はＤＡＴ）からＭＤ（又はＤＡＴ）へのデータコピーを行うに当たり、そのデータヘッドにコピー情報が付加されている。このコピー情報は２ビットからなるデータで、マスターディスクにおけるコピー情報が”００”の場合は、コピーを取ってもコピー情報は”００”のままであり、自由なコピーが可能である。

【０００６】一方、マスターディスクにおけるコピー情報が”１０”の場合は、子供のコピー（例えば、マスターディスクから一世代下のディスクのコピー）は可能であるが、孫のコピー（例えば、マスターディスクから二世代下のディスクのコピー）は不可能である。つまり、この場合は、コピーの際、このコピー情報がカウントアップされて”１１”となる。これが子供のコピーである。そして各システムはコピー情報が”１１”の場合はコピーできないように構成されており、孫のコピーを防止するようになっている。

【０００７】以上のシステムは、著作権保護のための不正なコピーを防止すべく構成された正当な機器を使用した場合の不正コピー防止方法である。しかし、各機器に不正コピー防止の対策が施されていても、機器間でデータを転送する際にその伝送路上で不正者によりデータが横流しされてしまったのでは、上記対策も無意味なものとなる。

【０００８】このような場合に対応し、従来から秘密性を要するデータを通信する際には、これを暗号化して送信することが広く行われている。暗号化方式には、大きく別けて公開鍵方式と秘密鍵方式があるが、上記場合のように処理の高速性が要求されるときは、秘密鍵を用いるのが一般的である。この秘密鍵を用いて暗号化を行う場合には、予めどの秘密鍵を用いて暗号化を行うか、通信者間で定めておき特定の秘密鍵を用いて暗号通信を行っている。

【０００９】

【発明が解決しようとする課題】このため秘密鍵が第三者に、例えば攻撃による秘密鍵の特定による盗用などによる漏洩があると、それが発覚した場合に、再度使用する秘密鍵を通信者間で更新する必要がある。したがって、より有効な機器間伝送における暗号化の方式が要望されている。

【００１０】また、不当なコピーデータに対しては、これを有効に再生させないような仕組みが必要である。また、上記ＳＣＭＳによる不正コピーの管理では、子供のコピーはいくらでも取れるので、子供のコピーからのコピー（孫コピー）をとることはできなくとも、悪意の不正者により子供のコピーが大量に作成される場合がある。さらに、ＳＣＭＳでは、コピー情報自体が不正者によって例えば”００”に書き換えられると、以降の不正コピーは自由に行われることになる。

【００１１】したがって、著作権の問題がさらに深刻となる大容量デジタル記録再生機器の場合には、ＳＣＭＳよりも確実で、かつ、きめ細かなコピー管理を実現可能なコピー管理方法が求められている。

【００１２】本発明は、このような実情を考慮してなされたもので、その第１の目的は、データ内のコピー管理を行う部分に対する不正者の攻撃を確実に防御できる不正データコピー防止装置及び方法並びに記録媒体を提供することにある。

【００１３】また、第２の目的は、不正なコピーデータを有効に再生させないようにする不正データコピー防止装置及び方法を提供することにある。さらに、第３の目的は、きめ細かなコピー管理を実現可能な不正データコピー防止装置及び方法を提供することにある。

【００１４】

【課題を解決するための手段】上記課題を解決するために、請求項１に対応する発明は、デジタルデータをコピーする機器に用いられる不正データコピー防止装置において、デジタルデータは、暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と有し、コピー管理情報の内容が所定の条件を満たして、デジタルデータがコピー不許可と判定されたときには、デジタルデータのコピーを行わな

い不正データコピー防止装置である。

【００１５】本発明はこのような手段を設けたので、データ内のコピー管理を行う部分，すなわちコピー管理情報に対する不正者の攻撃を確実に防御することができる。また、請求項２又は６に対応する発明は、デジタルデータをコピーする機器に用いられる不正データコピー防止装置又は方法において、デジタルデータは、暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、データ本体を復号するための鍵情報とを有し、コピー管理情報の内容が所定の条件を満たして、デジタルデータがコピー不許可と判定されたときには、デジタルデータ内の鍵情報を変更する鍵変更手段を備えた不正データコピー防止装置又は方法である。

【００１６】本発明はこのような手段を設けたので、不正なコピーデータを有効に再生させないようにすることができる。すなわちデジタルデータがコピー不許可と判定されたときには、デジタルデータ内の鍵情報が変更され、そのコピーされたデジタルデータは有効な再生ができないことになる。

【００１７】さらに、請求項３に対応する発明は、請求項１又は２に対応する発明において、コピー管理情報は、デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報と、当該デジタルデータを何回コピーしたかを示すコピー回数管理情報からなり、世代管理情報が所定の世代数となり、コピー回数管理情報が所定のコピー回数となると、コピー不許可であることを示す不正データコピー防止装置である。

【００１８】本発明はこのような手段を設けたので、請求項１又は２に対応する発明と同様な作用効果が得られる他、きめ細かなコピー管理を実現することができる。さらにまた、請求項４に対応する発明は、請求項１又は２に対応する発明において、コピー管理情報は、デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報を有し、当該世代管理情報が所定の世代数となるとコピー不許可であることを示すものであり、かつ、その情報ビット数を３ビット以上として、最初のデータのコピーのコピー以上の世代のデータまでコピー許可管理可能とした不正データコピー防止装置である。

【００１９】本発明はこのような手段を設けたので、請求項１又は２に対応する発明と同様な作用効果が得られる他、きめ細かなコピー管理を実現することができる。一方、請求項５に対応する発明は、請求項１～４に対応する発明において、デジタルデータを送信機器と受信機器間で伝送する場合であり、かつ送信機器又は受信機器に適用される不正データコピー防止装置であって、送信機器と受信機器と間で共有された一時鍵を暗号鍵もしくは復号鍵として、両者間で伝送されるデジタルデータを暗号化もしくは復号化する暗号化手段もしくは復号化手段を備えた不正データコピー防止装置である。

【００２０】本発明はこのような手段を設けたので、請求項１～４に対応する発明と同様な作用効果が得られる他、たとえデジタルデータ自体がデータ伝送中に不正コピーされても、伝送中はさらに暗号化されているので、不正者の不正利用を防止することができる。

【００２１】また、請求項７に対応する発明は、デジタルデータをコピーする機器に用いられる不正データコピー防止方法において、デジタルデータが最初のデータから何回目のコピーであるかを示す世代管理情報と、当該デジタルデータを何回コピーしたかを示すコピー回数管理情報からなるコピー管理情報をデジタルデータに付加し、世代管理情報が所定の世代数となり、コピー回数管理情報が所定のコピー回数となると、コピー不許可として不正なデータコピーを防止する不正データコピー防止方法である。

【００２２】本発明はこのような手段を設けたので、きめ細かなコピー管理を実現することができる。次に、請求項８に対応する発明は、暗号化されたデータ本体と、当該データ本体のコピー許可について管理する暗号化されたコピー管理情報と、データ本体を復号するための鍵情報と、コピー管理情報を復号するための鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体である。

【００２３】本発明はこのような手段を設けたので、コピー管理情報に対する不正者の攻撃を確実に防御することができる。ここで、コンピュータ読み取り可能な、としているが、ここでいうコンピュータはいわゆる計算機のみならず、デジタル再生記録機器等のあらゆる情報処理装置を含むものである。

【００２４】また、請求項９に対応する発明は、暗号化されたデータ本体と、データ本体を復号するためのデータ暗号鍵が当該データ暗号鍵を暗号鍵として暗号化されてなる第１の鍵情報と、データ暗号鍵が複数の暗号鍵によりそれぞれ暗号化されてなる複数の第２の鍵情報と、データ本体のコピー許可について管理するコピー管理情報が、複数の暗号鍵によりそれぞれ暗号化されてなる複数の第３の鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体である。

【００２５】本発明はこのような手段を設けたので、コピー管理情報に対する不正者の攻撃をより一層確実に防御することができる。ここで、コンピュータ読み取り可能な、としているが、ここでいうコンピュータはいわゆる計算機のみならず、デジタル再生記録機器等のあらゆる情報処理装置を含むものである。

【００２６】さらに、請求項１０に対応する発明は、暗号化されたデータ本体と、データ本体を復号するためのデータ暗号鍵が当該データ暗号鍵を暗号鍵として暗号化されてなる第１の鍵情報と、データ暗号鍵が複数の暗号鍵によりそれぞれ暗号化されてなる複数の第２の鍵情報

と、データ本体のコピー許可について管理するコピー管理情報が、データ暗号鍵を暗号鍵として暗号化されてなる第３の鍵情報とを有するデータ構造体が記録されたコンピュータ読み取り可能な記録媒体である。

【００２７】本発明はこのような手段を設けたので、コピー管理情報に対する不正者の攻撃をより一層確実に防御することができる。ここで、コンピュータ読み取り可能な、としているが、ここでいうコンピュータはいわゆる計算機のみならず、デジタル再生記録機器等のあらゆる情報処理装置を含むものである。

【００２８】

【発明の実施の形態】以下、本発明の実施の形態について説明する。本明細書では、暗号に関する技術について説明するが、以降、暗号化の操作をＥｙ(ｘ) と表す。ここで、ｘは暗号化の対象となるデータで、ｙは暗号化に用いる暗号鍵である。また復号化の操作をＤｙ(ｚ) と表す。ここで、ｚは復号の対象となるデータで、ｙは復号化に用いる復号鍵である。従って、

Ey(Dy(x))＝x

Dy(Ey(x))＝x

である。

【００２９】また、本実施形態を説明する図において、一点鎖線は暗号化または復号化のための鍵情報を表し、実線は暗号化または復号化の対象となる情報を表している。

（発明の第１の実施の形態）図１は本発明の第１の実施の形態に係る不正データコピー防止装置を適用するデジタル記録再生機器の接続構成例を示すブロック図である。

【００３０】同図では、ケーブルテレビ網を利用して音声／画像／文字などのマルチメディア情報が配信され、ＳＴＢ（Ｓｅｔ　Ｔｏｐ　Ｂｏｘ）１０１へ入力される例を示している。

【００３１】このシステムは、ＳＴＢ１０１がＩＥＥＥ１３９４ケーブル１０２を介してデジタルＶＣＲ１０３に接続されるとともに、デジタルＶＣＲ１０３からＩＥＥＥ１３９４ケーブル１０４，１０５を介してそれぞれディスプレイ１０６とＤＶＤ－ＲＡＭ１０７に接続され構成されている。同システムでは複数のデジタル記録再生機器が接続されているので、基本的には機器間でデータ送信、コピー等が可能である。

【００３２】このシステムでは、ＳＴＢ１０１、デジタルＶＣＲ１０３又はＤＶＤ－ＲＡＭ１０７がデータの送信機器になるものであり、一方、デジタルＶＣＲ１０３又はＤＶＤ－ＲＡＭ１０７がデータの受信機器になるものである。本実施形態では、これら各送信機器、受信機器間での不正なデータコピーを防止する方法について説明する。

【００３３】なお、上記構成について説明すると、まず、ＳＴＢ１０１はマルチメディアデータのスクランブルを解いたり（あるいはデシャッフリング）課金情報などの蓄積／送信を行うためのものである。ＳＴＢ１０１へ入力されたマルチメディアデータは、ＩＥＥＥ１３９４ケーブル１０２，１０４，１０５を介して各機器１０３，１０６，１０７に接続されているが、ＩＥＥＥ１３９４とは高速シリアルデジタルインターフェースで、ＩＥＥＥで制定されたものである。このインターフェースでは高速通信が可能で２種類のデータ転送、Ａｓｙｎｃｈｒｏｎｏｕｓ（非同期）とＩｓｏｃｈｒｏｎｏｕｓ（等時）ができる。このため、パーソナルコンピュータやデジタルテレビ、デジタルＶＣＲ、ＤＶＤ－ＲＡＭなどのデジタルＡＶ機器との接続に利用されるものである。

【００３４】次に本実施形態の不正データコピー防止方法を実現するためのデータ構造について説明する。図２は本実施形態に使用されるデータ構造の構成方法を説明する図である。

【００３５】ＤＶＤ等に格納されるデータは、タイトルキーやディスクキーを用いてコンテンツを暗号化する。本実施形態では簡単化のためコンテンツはディスクキーと呼ばれるデータ暗号鍵Ｄｋ で暗号化されることとする。図２において暗号化回路２０４によってデータがデータ暗号鍵Ｄｋ で暗号化されＥＤｋ （データ）となる様子が示されている。このデータ暗号鍵Ｄｋ は事前にデジタル記録再生機器製造メーカに知らされることはない。

【００３６】また、デジタル記録再生機器において画像等のデータを再生すべく上記データ暗号鍵Ｄｋ が暗号化されてデータ構造の一部として付加される。この暗号化されたデータ暗号鍵Ｄｋ は２種類用意される。その１つはデータ暗号鍵Ｄｋ 自体を暗号鍵としてデータ暗号鍵Ｄｋ を暗号化するもので、暗号化回路２０３により当該暗号化されＥＤｋ （Ｄｋ ）となる。もう１つは、データ暗号鍵Ｄｋ をマスター鍵束Ｍｋｎの各マスター鍵でそれぞれ暗号化する場合で、暗号化回路２０２により鍵束の鍵数だけ暗号化データＥＭｋ１（Ｄｋ ），ＥＭｋ２（Ｄｋ ），．．．，ＥＭｋｎ（Ｄｋ ）が生成される。

【００３７】このマスター鍵束Ｍｋｎは、例えば鍵管理会社によって管理されるものであり、デジタル記録再生機器製造メーカはこの鍵管理会社からマスター鍵束Ｍｋｎの一部分であるマスター鍵束Ｍｋｓが与えられる。このマスター鍵束Ｍｋｓはメーカにより異なる複数個のマスター鍵からなるものであり、これにより鍵管理がなされることになる。すなわち各メーカはマスター鍵Ｍｋ１，Ｍｋ２，．．，Ｍｋｎのうち少なくともその一部を所有しているので、データ構造の中に暗号化データＥＭｋ１（Ｄｋ），ＥＭｋ２（Ｄｋ ），．．．，ＥＭｋｎ（Ｄｋ ）と、ＥＤｋ （Ｄｋ ）とが含まれていれば、安全確実なデータ暗号鍵Ｄｋ の取出しが可能になる。データ暗号鍵Ｄｋ取出方法の詳細は後述する。

【００３８】本発明は、データコピーの安全な管理を行

うために、データ構造の中に、コピー管理フラグＣＦを暗号化して含めるようにしている。図２においてコピー管理フラグＣＦがマスター鍵束Mknによって暗号化回路２０１において暗号化され、暗号化データ列ＥMk1（ＣＦ），ＥMk2（ＣＦ），．．．，ＥMkn（ＣＦ）が生成される様子が示される。

【００３９】図３は本実施形態の不正データコピー防止装置に用いられるデータ構造例を示す図である。同図には、図２で説明した各暗号化データが組み合わされてデータ構造をなした様子が示されている。すなわち各マスター鍵で暗号化されたコピー管理フラグＣＦとデータ暗号鍵Dk のペア２１１が順次並べられマスター鍵暗号化部２１２が構成され、マスター鍵暗号化部２１２の後ろにＥDk （Dk ）であるディスク鍵暗号化部２１３が付加されている。そしてディスク鍵暗号化部２１３の後ろにＥDk （データ）であるデータ本体２１４が設けられ、データ構造体２１５が構成されている。

【００４０】なお、上記したように、データ本体２１４はデジタル化された文書、音声、画像あるいはプログラム等のデータが暗号化されたものであり、このデータ本体２１４にデータ暗号鍵Dk 及びコピー管理フラグＣＦが含まれてなるデータ構造体２１５が、そのまま又はさらに加工された形で、ＤＶＤ－ＲＡＭ１０７やＤ－ＶＣＲに記憶され、また、ネットワーク等を介してＳＴＢ１０１に送られてくる。すなわち、このデータ構造体２１５の形で送信や記録媒体への記録によるユーザ配布，販売を行う。

【００４１】そして、本発明は、このデータ構造体２１５に含まれているＣＦ，すなわち暗号化されて外部からの攻撃に耐え得るコピー管理フラグＣＦを利用して、データのコピー管理（世代管理、複写回数管理）を行い、不正なコピーデータを有効に再生させないようにするものである。

【００４２】以下、上記データ構造体２１５を扱うデジタル記録再生機器において、いかにしてデータ再生、データコピー等が行われるかについて具体的に説明する。図４は本実施形態の不正データコピー防止装置を用いたデジタル記録再生機器の構成例を示す図である。

【００４３】同図においては、送信機器３０１としてＤＶＤ－ＲＡＭ、受信機器３０２としてＤ－ＶＣＲを用い、両機器３０１，３０２をＩＥＥＥ１３９４ケーブル３０３で接続した場合を例にとって説明する。説明の都合上、送信機器３０１，受信機器３０２には送信受信用の構成のみを示すが、各機器には送信受信用の両構成が含まれている。また、送信機器３０１，受信機器３０２としては、図１に示したように種々の組み合わせた考えられるものである。

【００４４】送信機器３０１は、ＩＥＥＥ１３９４チップ３１１と、ＤＶＤ－ＲＡＭ３１２からデータ構造体２１５の形で保存されるデータを読み出し、またデータ書き込みを行う読出書込回路３１３とから構成されている。さらに、ＩＥＥＥ１３９４チップ３１１には、ＩＥＥＥ１３９４インターフェース処理を行い受信機器３０２と通信するＩＥＥＥ１３９４Ｉ／Ｆ部３１４と、鍵共有回路３１５，暗号化回路３１６，ＣＦ変更部３１７が設けられている。

【００４５】一方、受信機器３０２は、ＩＥＥＥ１３９４チップ３２１，３２２と、再生データに画質調整等を施しＩＥＥＥ１３９４チップ３２２を介してディスプレイ３０４にて表示させる表示処理部３２３と、ＩＥＥＥ１３９４チップ３２１のデータ再生コピー処理部３３４から出力されるデータ構造体２１５をＤＶカセット３２４に保存する書込処理部３２５と、ＤＶカセット３２４からデータ構造体２１５を読み出してデータ再生コピー処理部３３４に入力する読出処理部３２６とによって構成されている。ＩＥＥＥ１３９４チップ３２１には、ＩＥＥＥ１３９４インターフェース処理を行い送信機器３０１と通信するＩＥＥＥ１３９４Ｉ／Ｆ部３３１と、鍵共有回路３３２，復号化回路３３３，データ再生コピー処理部３３４が設けられている。

【００４６】上記各構成のうち、鍵共有回路３１５，３３２と、暗号化回路３１６と復号化回路３３３とは、データ構造体２１５をＩＥＥＥ１３９４ケーブル３０３上で伝送させる際に、これを暗号化させるための構成である。

【００４７】鍵共有回路３１５及び３３２は、ＩＥＥＥ１３９４ケーブル３０３での情報伝送により一時鍵Ｓtkを安全に共有するようになっている。また、暗号化回路３１６は、ＣＦ変更部３１７から出力されたＤＶＤ－ＲＡＭデータ（データ構造体２１５）に対し鍵共有回路３１５からの一時鍵Ｓtkを用いて暗号化を行う。さらに、復号化回路３３３は、鍵共有回路３３２からの一時鍵Ｓtkを用い、ＩＥＥＥ１３９４Ｉ／Ｆ部３３１から受け取った暗号化されたデータ構造体２１５を復号してデータ再生コピー処理部３３４に引き渡すものである。なお、一時鍵Ｓtkの鍵共有方式については、第４及び第５の実施形態でも詳しく説明する。

【００４８】送信機器３０１のＣＦ変更部３１７は、読出書込回路３１３で読み出されたデータ構造体２１５を暗号化回路３１６に引き渡すとともに、コピー管理フラグＣＦを変更し、そのＣＦの変更された新たなデータ構造体２１５でもってＤＶＤ－ＲＡＭ３１２内の同一データ構造体を更新する。

【００４９】受信機器３０２のデータ再生コピー処理部３３４は、復号化回路３３３又は読み出し処理部３２６から受け取ったデータ構造体２１５を自己のもつ鍵束Mksにより解読してデータ暗号鍵Dk 及びコピー管理フラグＣＦを取り出すとともに、データ暗号のとかれたデータを表示処理部３２３に出力する。また、コピー管理フラグＣＦを変更したのち、自己のマスター鍵束Mksを用

いてデータ構造体２１５を作成し、書込み処理部３２５に保存用データ（コピーデータ）として出力する。

【００５０】次に、以上のように構成された本発明の実施の形態に係る不正データコピー防止装置の動作について説明する。送受信間でデータ転送が行われることとなると、まず、送信機器３０１と受信機器３０２との間で、鍵共有回路３１５，３３２により一時鍵Ｓtkの共有化が行われる。

【００５１】次に、ＤＶＤ－ＲＡＭ３１２からデータ構造体２１５が読み出され、ＣＦ変更部３１７を介して暗号化回路３１６に入力され、ここでデータ構造体２１５の一時鍵Ｓtkによる暗号化が行われる。そして、暗号化

ＥMk1（Dk），ＥMk2（Dk），…，ＥMkn（Dk）　…２１５ａ
ＥMk1（ＣＦ），ＥMk2（ＣＦ），…，ＥMkn（ＣＦ）　…２１５ｂ
ＥDk(Dk)　；ディスク鍵暗号化部　…２１３
ＥDk（データ）　；データ本体　…２１４

にわけるようになっている。ＥDk（データ）以外は長さが決まっていて、図３のごとくヘッダとして付加された部分をわけることは容易である。

【００５４】さて、マスター鍵束Mknもしくは Mksを暗号鍵として暗号化されたデータ暗号鍵２１５ａは、図３のマスター鍵暗号化部２１２の一部であり、安全のためＩＥＥＥ１３９４チップの利用者が勝手に取り出せない領域に記憶される。このマスター鍵束で暗号化されたデータ暗号鍵２１５ａは、この装置製造メーカに供給されているマスター鍵束Mksを順に復号鍵として用いて復号される。

【００５５】このときＥMk1（Dk），ＥMk2（Dk），…，ＥMkn（Dk）２１５ａは、いったんメモリ４０２に取り込まれ、制御信号１にて受信機器のＩＥＥＥ１３９４チップ内のマスター鍵束Mksを順に復号鍵として取り出し復号化回路４０３にて、例えばＥMk1（Dk）から順に復号していく。

【００５６】復号して得られたDk′を復号鍵としてＥDk(Dk)を復号化回路４０４にて復号してDk″を得る。Dk′とDk″とを判定回路４０５で比較する。Dk′＝Dk″であるならば、データ暗号鍵を暗号化するのに用いたマスター鍵と、暗号化されたデータ暗号鍵を復号するのに用いたマスター鍵とが等しいことに他ならない。しかしDk′≠Dk″であるならば、データ暗号鍵を暗号化するのに用いたマスター鍵と、暗号化されたデータ暗号鍵を復号するのに用いたマスター鍵とが異なっているということである。さらに全てのマスター鍵についてDk′≠Dk″ならば、この暗号，例えばＥMk1（Dk）は、このチップの所有するマスター鍵束Mksでは解けないということである。

【００５７】このような場合には、制御信号２により次のＥMk2（Dk）をメモリ４０２から呼び出し、ＩＥＥＥ１３９４チップ内のマスター鍵束Mksを用いて、上記と同様の操作をDk′＝Dk″となるＥMkiが見つかるまで繰り返す。

【００５８】Dk′＝Dk″となれば、そのときのマスター鍵でＥMki（Dk）からデータ暗号鍵Dk が取り出せたことになる。そこで制御信号３によりメモリ４０６に記憶されているＥMk1（ＣＦ），ＥMk2（ＣＦ），…，ＥMkn（ＣＦ）のうち、ＥMki（ＣＦ）を取り出す。なお、マスター鍵束で暗号化されたコピー管理フラグ２１５ｂは、１からｎ（又はｓ）まで、マスター鍵束で暗号化されたデータ暗号鍵２１５ａと同じ並びになっているので、ＥMki（ＣＦ）の特定は容易である。

【００５９】次に、復号化回路４０７により特定されたマスター鍵を用いたＥMki（ＣＦ）の復号が行われＣＦが得られる。そしてＣＦ変更回路４０８にてコピー管理フラグＣＦが変更されてデータ更新回路４０９の暗号化回路４１０に入力される。

【００６０】このデータ更新回路４０９には、データ読取り制御回路からＥDK（データ），すなわちデータ構造体２１５におけるデータ本体２１４が入力されるようになっている。一方、Dk，変更されたＣＦも入力されるようになっており、暗号化回路４１０において、これらがマスター鍵束Mks及びデータ暗号鍵Dk によって暗号化され、データ本体２１４のヘッダとして付される。

【００６１】このメーカ毎のマスター鍵束Mksで暗号化され、かつ変更されたコピー管理フラグＣＦを有するデータ構造体２１５（MknがMksとなった他は、図３と同一構造）が読出書込回路３１３に出力され、この新たなデータ構造体でＤＶＤ－ＲＡＭ３１２の対応する部分が更新される。

【００６２】ここで、コピー管理フラグＣＦは世代管理情報と、コピー回数管理情報とからなっている。世代管理というのは、マスターディスクから子供コピー、さらに孫コピーを作るように新世代を作る場合のコピー管理である。一方、コピー回数管理というのは、そのデータ構造体で何回コピーを行ったかを管理するものである。

この場合、ＣＦ変更部３１７を通過して暗号化回路３１６に引き渡されたデータ構造体２１５はその受け取り先で世代管理がなされることとなり、一方、ＣＦ変更部３１７により、ＤＶＤ－ＲＡＭ３１２に戻され更新されるデータ構造体は、ＣＦ変更回路４０８にてコピー回数のみがカウントアップされて世代の変更は行われない。なお、カウント数が最大値となるとデータ送出先（受信機器３０２）において正常なデータコピーができなくなる。

【００６３】このようにして、送信機器３０１においてコピー管理がなされる一方、受信機器３０１においても受信したデータ構造体２１５についてのコピー管理が行われる。以下、受信側での処理を説明する。

【００６４】まず、受信機器３０２のＩＥＥＥ１３９４Ｉ／Ｆ部３３１で受け取った暗号化されたデータ構造体は、鍵共有回路３３２から与えられる一時鍵Ｓｔkにより復号化回路３３３にて復号され、データ再生コピー処理部３３４に入力される。

【００６５】図６は本実施形態のデータ再生コピー処理部の構成及びその処理を示す図であり、図５と同一部分には同一符号を付する。データ再生コピー処理部３３４に入力されるデータ構造体２１５は、まずデータ読取り制御回路４０１に入力され、図５のＣＦ変更部３１７の場合と同様にわけられる。以下、判定回路４０５にてデータ暗号鍵Dk が取り出され、さらに、復号化回路４０７にてコピー管理フラグＣＦが取り出されるまでは、図５のＣＦ変更部３１７と同様な処理が行われる。

【００６６】次に、取り出されたコピー管理フラグＣＦの状態がＣＦ判定回路４１１にて判定される。コピー管理フラグＣＦの世代管理及びコピー回数管理の具体的な内容は後述する。ここで、コピー管理フラグＣＦがこれ以上コピーできない世代にあるか否か、たとえ次世代コピーが許される世代であってもそのデータ構造体のコピー可能な最大回数に達しているか否かが判定されることで、コピー可否が判断される。そして、ＣＦ判定回路４１１によりコピー管理フラグＣＦ及びコピー可否の判定結果（制御信号４）が鍵変更回路４１２に与えられる。

【００６７】鍵変更回路４１２は、記録コマンドや再生コマンドあるいはその両方がユーザから入力されていることを知らせる制御信号５にて、コピー管理フラグＣＦと、先に得られたデータ暗号鍵Dk をそのままあるいは変更して出力するようになっている。

【００６８】データ再生を行い、単にディスプレイ３０４に表示する場合には、データ構造体２１５のデータ本体２１４たるＥDk （データ）が復号化回路４１３で復号化されてデータとして取り出されて表示処理部３２３に出力される。このとき、鍵変更回路４１２から復号化回路４１３には、常に判定回路４０５で取り出されたデータ暗号鍵Dk が復号化鍵として与えられる。したがって、正常なデータ暗号鍵Dk が取り出される限りは、コピー管理フラグＣＦの状態にかかわらず、データ再生だけは正常に行われる。

【００６９】これに対して、ＤＶカセット３２４にデータコピーを行う場合には、ＣＦ判定回路４１１での判定結果によりその処理が異なることになる。まず、コピー管理フラグＣＦがコピー可能な状態にある場合について説明する。このときには、鍵変更回路４１２からは、コピー管理フラグＣＦがＣＦ変更回路４１４に入力され、一方、データ暗号鍵Dk が暗号化対象データとしてかつ暗号化鍵としてコピー回路４１５の暗号化回路４１６に入力される。

【００７０】ＣＦ変更回路４１４では、世代の変更が行われる。すなわちコピー管理フラグＣＦの世代管理情報が変更され、データ構造体が次世代のものとされる。この変更されたコピー管理フラグＣＦは、コピー回路４１５に入力される。

【００７１】つまり、コピー回路４１５には、データ構造体のデータ本体２１４としてのＥDk （データ）がデータ読取り制御回路４０１から入力され、さらにDk 及び変更されたＣＦが入力されている。暗号化回路４１６では、Dk 及びＣＦがマスター鍵束Mks及びデータ暗号鍵Dk によって暗号化され、データ本体２１４のヘッダとして付される。

【００７２】このメーカ毎のマスター鍵束Mksで暗号化され、かつ変更されたコピー管理フラグＣＦを有するデータ構造体２１５（MknがMksとなった他は、図３と同一構造）が書込み処理部３２５に出力され、ＤＶカセット３２４にコピーデータとして格納される。なお、このコピー操作でマスター鍵束がMknからMksとなっているので、以降、保存されたデータ構造体２１５は、このメーカ互換性がなくなり、マスター鍵束Mksをもたない機器では再生やコピーができなくなる。

【００７３】また、この保存されたデータ構造体２１５を再生する場合には、読出処理部３２６からマスター鍵束Mksで暗号化されたデータ構造体がデータ読取り制御回路４０１に入力され、上記と同様な処理がなされる。

【００７４】次に、コピー管理フラグＣＦがコピー可能な状態にない場合について説明する。このときデータ構造体はすでにコピーできない状態にあるので、ＣＦ変更回路４１４では特にコピー管理フラグＣＦの変更はなされない。一方、鍵変更回路４１２から暗号化回路４１６へのデータ暗号鍵の出力がコピー可能な場合とは異なったものとなる。

【００７５】すなわちコピー不可の場合、鍵変更回路４１２は、暗号化対象データかつ暗号化鍵となるデータ暗号鍵として、判定回路４０５で取り出された正規のデータ暗号鍵Dk とは異なる偽のデータ暗号鍵Dk*を暗号化回路２１５に入力する。Ｄｋを変更して偽のＤｋ＊を作るには、例えばDk のビットを反転するとか、ビットシフトを行うとか、ある特定の数値との排他論理和をとる

などの演算を行う、といった方法がある。

【００７６】なお、各データを与えられたコピー回路４１５及び暗号化回路４１６の処理は上記と同様である。しかしながら、この回路４１５で生成され保存されたデータ構造体２１５においては、図３におけるＥＤｋ（データ）の暗号鍵はＤｋのままで、ヘッダ部であるマスター鍵暗号化部２１２及びディスク鍵暗号化部２１３に使用され格納されるデータ暗号鍵Ｄｋ*はすべてにせものとなっている。したがって、このデータ構造体を復号するときには、偽のデータ暗号鍵Ｄｋ*が取り出され、偽のデータ暗号鍵Ｄｋ*によるでたらめなデータ再生が行われることになる。

【００７７】以上が送信機器３０１から受信機器３０２へデータ構造体２１５をコピーし、またデータ再生する場合の処理である。すなわち送信機器３０１で元データに対するデータコピーの回数管理が行われ、受信機器３０２にて受け取りデータをコピーすることによるデータコピーの世代管理が行われている。

【００７８】次に、コピー管理フラグＣＦの具体的な内容及び世代管理、コピー回数管理について図７、図８を用いて説明する。図７はコピー管理フラグＣＦの構成例を示す図である。本実施形態では、８ビットを１バイトとして、上位３ビットをコピー世代の管理のためのビット（世代管理情報）とし、下位５ビットをコピー回数を管理するためのビット（コピー回数管理情報）としている。

【００７９】図８はコピー世代の管理ビットの状態遷移を表した図である。コピー世代管理ビットは、

０００…コピー可能

００１…子コピー可能（孫コピーは不可）→子は１１１になる

０１１…孫コピー可能（曾孫コピーは不可）→子は００１になり、孫は１１１になる

１１１…コピー不可

とする。従って図８のごとく、コピー世代管理ビットがオール０の場合は、コピーをしてもオール０のままであるが、コピー世代管理ビットが“００１”である場合は、子供のコピーは可能であるが、孫のコピーは不可としているため、コピーをすると子供のコピーのコピー世代管理ビットは“１１１”となり、コピー不可となる。一方、コピー世代管理ビットが“０１１”である場合は、孫コピーまで可能であるので、子供のコピーのコピー世代管理ビットは“００１”となり、孫コピーのコピー世代管理ビットは“１１１”となってコピー不可となる。こうして、コピー世代を管理するものとする。

【００８０】また、コピー回数は、コピー回数管理ビットが最大値になると、たとえコピー世代管理ビットがコピー可能な世代であってもコピー不可となる。本実施形態ではコピー回数管理ビットが５ビットであるため、１回から３２回までの回数管理しかできないが、ビット数を増やせば、さらに多くの回数管理が可能である。

【００８１】回数管理の場合、例えばソフトウェアのマスターディスクのユーザ数を制限する場合などに利用が可能である。マスターディスクのコピー世代管理フラグは子供のコピーが可能な“００１”としておく。こうすれば、ユーザがコピーしたソフトウェアを更にコピーされることを防ぐことが可能である。

【００８２】コピー回数管理ビットは、マスターディスクからコピーできるユーザ数を表しており、本実施形態の場合、０～３２人までコピーすることが可能である。例えば、マスターディスクからコピー可能なユーザ数を１０人とする。この場合、最初のコピー回数管理ビットは“０１０１０”である。一人がコピーすると、

マスターディスクのＣＦ：　００１０１００１

ユーザのＣＦ　　：　１１１００００

となり、ユーザがコピーしたソフトウェアは、他媒体へ記録ができなくなる。

【００８３】こうして、１０人のユーザがソフトウェアをコピーすると、

マスターディスクのＣＦ：　００１００００

となり、子供のコピーが可能のままであるが、回数が０回であるため、これ以上のコピーは許可されない。

【００８４】なお、最後の人がコピーをした時点でマスターディスクのコピー世代管理ビットを“１１１”にしておく方法もある。上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、コピー管理フラグＣＦを暗号化してデータ構造体２１５に含ませるようにしたので、コピー管理フラグＣＦを伝送途中で書き換えて不正コピーすることを防止でき、コピー管理フラグＣＦに対する不正者の攻撃を確実に防御できる。これにより著作権を確実に保護することができる。

【００８５】また、データ再生コピー処理部３３４にＣＦ判定回路４１１及び鍵変更回路４１２を設けてコピーできないデータ構造体をコピーするときには、データ暗号鍵を変更するようにしたので、不正なコピーデータを有効に再生させないようにすることができる。

【００８６】また、ＣＦ変更部３１７を設けて、コピーのために伝送するデータ構造体のコピー回数をカウントアップさせることができ、きめ細かで効果的なコピー管理を実現することができる。

【００８７】さらに、データ再生コピー処理部３３４にＣＦ判定回路４１１及びＣＦ変更回路４１４を設けてコピー対象となるデータ構造体の世代を進めるようにしたので、きめ細かで効果的なコピー管理を実現することができる。

【００８８】また、鍵共有回路３１５，３３２及び暗号化回路３１６を設け、伝送されるデータ構造体を暗号化するようにしたので、受信側に復号化回路３３３を備えていなければ当該データを利用できないようにすることができる。また、機器間を一時的な暗号鍵で暗号化して

伝送を行うため、機器間を接続するケーブルから他記録媒体に記録して再利用する不正なコピーを防止することができる。

【００８９】さらに、コピーが可能か否かを示すためのコピー管理フラグＣＦには、コピーが何世代まで可能かを示す部分と、コピー回数が何回まで可能かを示す部分とを設けたので、コピーの世代管理と回数管理により、きめ細かなコピー許可不許可管理を行うことができる。

【００９０】なお、本実施形態では、ＣＦ変更部３１７、データ再生コピー処理部３３４は、それぞれＩＥＥＥ１３９４チップ３１１，３２１に含まれる構成としたが、本発明はこのような構成に限られるものでなく、例えばＣＦ変更部３１７、データ再生コピー処理部３３４が別チップとなる構成としてもよい。

（発明の第２の実施の形態）本実施形態では、不正データコピー防止方法を実現するための他のデータ構造について説明する。

【００９１】図９は本発明の第２の実施形態に使用されるデータ構造の構成方法を説明する図であり、図２と同一部分には同一符号を付して説明を省略する。図９においては、コピー管理フラグＣＦを暗号化する暗号化鍵にデータ暗号鍵Dk が用いられる他、各データの暗号化は第１の実施形態と同様である。ただし、図２ではマスター鍵束が使用される関係上、ＣＦの暗号化データは複数となったが、本実施形態では、データ暗号鍵Dk が用いられるので、ＣＦの暗号化データは１つである。

【００９２】図１０は本実施形態の不正データコピー防止装置に用いられる他のデータ構造例を示す図である。同図には、図９で説明した各暗号化データが組み合わされてデータ構造をなした様子が示されている。すなわちこのデータ構造体２２６では、データ暗号鍵Dk で暗号化されたコピー管理フラグ部２２１と、マスター鍵で暗号化されたデータ暗号鍵２２２が順次並べられたマスター鍵暗号化部２２３と、EDk （Dk ）であるディスク鍵暗号化部２２４とが順次並べられヘッダ部となっている。そして、EDk （データ）であるデータ本体２２５の先頭に、このヘッダ部が設けられ、データ構造体２２６として構成されている。

【００９３】このようなデータ構造体２２６は、データコピーのコピー管理、不正コピー防止を実現するべく不正データコピー防止装置を備えたデジタル記録再生機器において記録再生用データとして使用される。

【００９４】その適用対象は、第１の実施形態で説明したデジタル記録再生機器と同様である。すなわち、データ構造体２２６は、データ読取り制御回路における振り分け対象が一部変更され、ＣＦを暗号復号する鍵がDk になっている他は、図１、図４、図５、図６に示した各装置において利用できる。

【００９５】なお、データ構造体２２６を用いた場合の図６に対応したデータ再生コピー処理部３３４ｂの構成を図１１に示す。図１１は本実施形態の不正データコピー防止装置のデータ再生コピー処理部の構成及びその処理を示す図であり、図６と同一部分には同一符号を付する。なお、不正データコピー防止装置を含むシステムの全体構成は図４に示す場合と同様である。

【００９６】同図において、第１の実施形態（図６）との相違点は、データ読取り制御回路４０１にデータ構造体２２６が入力され、そのデータ振り分けにより、EDk （ＣＦ）をメモリ４０６に入力しマスター鍵暗号化部２２３をデータ本体２２５とともにコピー回路４１５ｂに入力することと、復号化回路４０７で使用される復号化鍵が、判定回路４０５で得られたデータ暗号鍵Dk となっていることと、また、コピー回路４１５ｂにおいては各部からの入力により、データ構造体２１５ではなくデータ構造体２２６を生成することである。なお、コピー回路４１５ｂにおいてはデータ読取り制御回路４０１から入力されたマスター鍵暗号化部２２３がデータ構造体２２６のヘッド部の一部にそのまま利用される。なお、コピー不可時にDk がDk*に変更された場合、EDk*（Dk*）となる新たなディスク鍵暗号化部２２４のDk*がDk と異なっているので、このデータ構造体のマスター鍵暗号化部２２３からデータ暗号鍵Dk が取り出されることはない。

【００９７】この結果、コピー回路４１６から出力されるデータ構造体２２６は、ＣＦが変更されあるいは不正コピー時にDk*が変更される他、データ再生コピー処理部３３４ｂに入力されたデータ構造体２２６のままである。特にマスター鍵暗号化部２２３がメーカ毎のマスター鍵束Mksで置き換えられることがないので、コピーされたデータはメーカ互換性を失うことはない。

【００９８】なお、本実施形態で使用される送信側のＣＦ変更部も、上記図６～図１１間と同様な変更が図５に示すＣＦ変更部３１７に施される（図示せず）。すなわち復号化回路４０７に復号鍵としてデータ暗号鍵Dk が入力され、データ更新回路４０９にマスター鍵暗号化部２２３が入力されて更新用のデータ構造体２２６のヘッド部に利用される。したがって、コピー回数管理時においてもデータ構造体２２６はメーカ互換性を失わない。

【００９９】上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、第１の実施形態と同様な構成を設けた他、デジタルデータとしてデータ構造体２２６を使用するようにしたので、第１の実施形態と同様な効果が得られる他、データコピーを行う際に、最初のマスター鍵束Mknで暗号化されたデータ暗号鍵をそのまま残すことができ、コピーデータやコピー元のデータのメーカ互換性を失わないようにすることができる。

（発明の第３の実施の形態）第１又は第２の実施形態では、図３に示すデータ構造体２１５又は図１０に示すデータ構造体２２６のみがシステムで使用される場合につ

いて説明した。しかし、実際の使用においては、これらの各データ構造体が混在する場合も考えられる。本実施形態では、このような場合の対応方法について説明する。

【０１００】図１２は本発明の第３の実施形態の不正データコピー防止装置に用いられる他のデータ構造例を示す図である。同図（ａ）は、データ構造体２１５の先頭に識別ビット２３１ａを付加し、データ構造体２１５ｂとしたものを示す。

【０１０１】一方、同図（ｂ）は、データ構造体２２６の先頭に識別ビット２３１ｂを付加し、データ構造体２２６ｂとしたものを示す。データ再生コピー処理部３３４，３３４ｂ、ＣＦ変更部３１７（第２実施形態の場合を含む）のデータ読取り制御回路４０１は、この識別ビット２３１ａ，２３１ｂを読み取って、各部に何れのデータ構造体に対応した処理を行うかの制御信号を出力する。

【０１０２】上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、第１又は第２の実施形態と同様な構成を設けた他、デジタルデータとしてデータ構造体２１５ｂ及び２２６ｂを使用するようにしたので、第１又は第２の実施形態と同様な効果が得られる他、異なる形式のデータ構造体を混在させても、それぞれのデータ構造に応じた処理を行うことができる。

（発明の第４の実施の形態）上記各実施形態では、データ構造体をいかなる構成とし、これに含まれるコピー管理フラグＣＦによりいかにしてデータコピー管理を行うかについて説明してきた。しかしながら、上記方法でデータコピー管理を行ってもデータ伝送路上でデータ構造体を不正に取得され、いわゆるデータ横流しをされてしまったのでは、上記データ管理方法の効果も減じることになる。これを防止すべく、上記各実施形態では、鍵共有回路３１５，３３２を設け、一時鍵Ｓtkを共有してこの一時鍵Ｓtkで暗号化されたデータを伝送路（ＩＥＥＥ１３９４ケーブル３０３）上で伝送させるようにしている。

【０１０３】本実施形態及び第５の実施形態では、この一時鍵Ｓtkを共有する方法について説明する。したがって、本実施形態及び第５の実施形態で以下に説明される鍵共有システムが第１，第２又は第３の実施形態における鍵共有回路３１５，３３２に用いられることになる。

【０１０４】図１３は本発明の第４の実施形態におけるマスター鍵束を利用した各機器間で一時暗号鍵を共有するための仕組みを説明した図であり、ネットワークまたはケーブルにより接続された機器間においてネットワークまたはケーブル上を流れる秘密情報を暗号化／復号化するための一時鍵の共有方法について図示したものである。本実施形態では、ＩＥＥＥ１３９４で接続された送信機器と受信機器との間で一時鍵を共有する場合について説明する。

【０１０５】同図において、送信機器５０１と受信機器５０３とがＩＥＥＥ１３９４ケーブル５０２によって接続されている。送信機器にマスター鍵の鍵束５０４ａ（Mks）が記録され、受信機器にマスター鍵の鍵束５０４ｂ（Mks）が記録されている。両者の鍵束は異なっていても構わないが、必ず鍵束の中の何個かは同じマスター鍵が含まれている必要がある。本実施形態では、両者のマスター鍵の鍵束（Mks）は同じであるものとする。

【０１０６】送信機器５０１の鍵共有にかかる部分は、一時鍵生成回路５０５と暗号化回路５０７ａ，５０７ｂによって構成される。一時鍵生成回路５０５は、ネットワークまたはケーブル上を流れるデータを一時的に暗号化するための一時鍵を生成するものである。この一時鍵生成回路５０５は、例えば特定の長さの乱数を生成する乱数発生器で行うことが好ましい。

【０１０７】一時鍵５０６（Ｓｋ）は一時鍵生成回路５０５で生成された鍵である。暗号化回路５０７ａは、マスター鍵の鍵束５０４ａの何れかで一時鍵５０６を暗号化する回路で、暗号化回路１０７ｂは一時鍵Ｓｋ を一時鍵Ｓｋ で暗号化するである。暗号化回路５０７ａと暗号化回路５０７ｂは暗号化方式が同じであれば同一の回路で構成しても構わない。ＥMki（Ｓｋ）５０８は暗号化回路５０７ａの出力で、ＥＳｋ （Ｓｋ）５０９は５０７ｂ暗号化回路の出力である。

【０１０８】一方、受信機器５０３の鍵共有にかかる部分は、復号化回路５１０ａ，５１０ｂと一時鍵判定回路５１３によって構成される。復号化回路５１０ａは、暗号化回路５０７ａの出力をマスター鍵の鍵束Mkiで復号する。復号化回路５１０ｂは、暗号化回路５０７ａの出力を復号回路５１０ａの出力で復号する。

【０１０９】Ska５１１は復号回路５１０ａの出力で、Ｓkb５１２は５１０ｂ復号回路の出力である。一時鍵判定回路５１３は復号化回路５１０ａの出力と復号化回路５１０ｂの出力とを比較判定する判定回路である。制御信号５１４は判定の結果によりマスター鍵の鍵束を変更するための信号で、Ｓｋ ５１５は判定の結果得られた一時鍵である。

【０１１０】次に、以上のように構成された本発明の実施の形態に係る一時鍵共有装置の動作について説明する。まず、もしマスター鍵が１つだけ存在するのであれば（これをMk0とする）、単に送信機器５０１にてMk0でＳｋ を暗号化し、このＥMk(Ｓk)を受信機器５０３へ送り、受信機器５０３にてMk0でＥMk(Ｓk)を復号化することにより、Ｓkを取り出すことができる。しかし、万一マスター鍵が破れた（漏洩した）場合、マスター鍵を交換しなければならず、新しい機器と古い機器とで互換性がなくなる可能性がある。

【０１１１】そこで本実施形態では、複数のマスター鍵からなる鍵束Mksのうちの使用したマスター鍵Mkiを直

接的に指し示す識別情報は送信機器５０１から受信機器５０３へは送らず、その代わりに、上記マスター鍵Mkiを特定可能とする情報（ここではＥMki（Sk）５０８及びＥSk（Sk）５０９を意味する）を送信機器５０１から受信機器５０３へ送り、受信機器５０３にてSkの暗号化に使用されたマスター鍵Mkiがマスター鍵のうちのいずれかであるかを特定するとともに、このマスター鍵の特定を通じてSkを得る。

【０１１２】図１４は本実施形態の動作を説明する流れ図である。まず、送信機器５０１において、受信機器５０３との間で共有される一時鍵５０６が一時鍵生成回路５０５で生成される（Ｓ１１）。

【０１１３】以下、図１４のステップＳ１２のより詳しい手順について説明する。生成されたSkはｎ個のマスター鍵（共通鍵暗号方式における共通鍵）の鍵束５０４ａのうちから例えばランダムあるいは順番に選んだ１つ（これをMkiとする）で暗号化される。すなわちMks（ｓ＝１，…，ｎ；ｎは２以上の整数）のうちいずれか１つのMkiで一時鍵Skを暗号化回路５０７ａで暗号化してＥMki（Sk)を得る。

【０１１４】このマスター鍵Mksはあらかじめ登録されているものであり、ユーザは見ることができない仕組みになっている。なお万一、マスター鍵が破られたことが発覚した場合、それ以降、送信機器にはその破られたものを除いてマスター鍵が作り込まれる。受信機器５０３側は、その破られたものを除いてマスター鍵が作り込まれてもよいし、そうしなくてもよい。ただし、ＩＥＥＥ１３９４の場合、どの機器が送信機器となるか受信機器となるか、区別がない（Ｄ－ＶＣＲやＤＶＤ－ＲＡＭなどの録画再生機器は、送信機器と受信機器とになりうる）ため、破られたマスター鍵を除いたものに換えることが望ましい。なお、全体の制御は図示しない各機器内の制御部が司るものとする。制御部は、例えばプログラムを各機器内に内蔵されたＣＰＵなどで実行することにより実現することができる。

【０１１５】さらに、暗号化回路５０７ｂによりSk自身を暗号鍵として用いてSkを暗号化してＥSk(Sk)を得る。そして、ＥMki（SK)とＥSk(Sk)を、ＩＥＥＥ１３９４ケーブル５０２を通じて受信機器５０３へ送る。

【０１１６】次に、受信機器５０３にて、まずマスター鍵を１つ選ぶ（これをMkpとする）。選んだMkpを復号鍵として、復号化回路５１０ａにより復号化し、

ＤMkp（ＥMki（Sk））＝Ska

を得る。

【０１１７】次に、復号化回路５１０ａからの出力Skaを復号鍵として復号化回路５１０ｂにより、ＥSk(Sk)を復号化し、

ＤSka（ＥSk(Sk)）＝Skb

を得る。

【０１１８】次に、一時鍵判定回路５１３により、SkaとSkbとが一致するか否か調べる。ここで、送信機器５０１にてSkを暗号化したマスター鍵MkiがMkpであったならば、

Ska＝ＤMkp（ＥMki（Sk））＝Sk

となり、従って、

Skb＝ＤSka（ＥSk(Sk)）＝ＤSk(ＥSk(Sk)）＝Sk

となり、ゆえに、

Ska＝Skb＝Sk

となる。

【０１１９】つまり、一時鍵判定回路５１３により、SkaとSkbとが一致することが判った場合には、

Mki＝Mkp、かつ、Ska＝Skb＝Sk

であり、この場合、一時鍵判定回路５１３は

Ska＝Skb＝Sk

を出力する。

【０１２０】一方、一時鍵判定回路５１３により、SkaとSkbとが一致しないことが判った場合には、

Mki≠Mkp

であり、送信機器５０１にてSkはこのMkpで暗号化されておらず、それ以外のマスター鍵で暗号化されたことがわかる。この場合、一時鍵判定回路５１３は出力をしないか、あるいは一時鍵判定回路５１３の出力は以後の処理部へ伝えられない。

【０１２１】以降は、SkaとSkbとが一致するまで、復号化に用いるMkpを変更して、上記の手順を繰り返す。例えば、最初にMkpとMk1を用いて上記の手順を行ってSkaとSkbとが一致しなかった場合に、次にMk2へと更新して再び上記の手順を繰り返すのである。

【０１２２】以上のような手順を用いて、送信機器５０１にてどのマスター鍵を用いたのかを受信機器５０３で特定することができるとともに、送信機器５０１と受信機器５０３との間で一時鍵Skを安全に共有することが可能となる。

【０１２３】上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、第１、第２又は第３の実施形態と同様な構成を設けた他、マスター鍵を用いて送信機器５０１と受信機器５０３との間で一時鍵Skを安全に共有することができるようにしたので、第１、第２又は第３の実施形態と同様な効果が得られる他、機器間を接続するケーブルから他記録媒体に記録して再利用する不正なコピーをより一層確実に防止することができる。

（発明の第５の実施の形態）本実施形態では、一時鍵を共有する他の方法，すなわちマスター鍵を用いずに一時鍵を共有する方法について、図１５と図１６を用いて説明する。

【０１２４】この方式は、「日経エレクトロニクス，Ｎｏ．６７６，ｐｐ．１３－１４，１９９６．１１．１

8」に開示された技術を応用したものである。図１５は本発明の第５の実施形態における鍵共有回路の構成例を示すブロック図である。

【０１２５】図１６はこの鍵共有回路によりマスター鍵束を用いずに各機器間で一時暗号鍵を共有するための仕組みを説明した図である。いま、ＩＥＥＥ１３９４で接続された機器にノードが割り振られ、図１６に示すようにノード＃１とノード＃２とで一時鍵を共有するものとする。まず図１５を用いて、本実施形態における鍵共有手順に用いる鍵共有回路６３０ａ，６３０ｂの構成について説明する。

【０１２６】鍵共有回路６３０ａは、チャレンジ鍵生成回路６３１ａ、認証鍵生成回路６３３ａ、比較回路６３５ａ、一時鍵生成回路６３７ａを備えている。同様に鍵共有回路６３０ｂは、チャレンジ鍵生成回路６３１ｂ、認証鍵生成回路６３３ｂ、比較回路６３５ｂ、一時鍵生成回路６３７ｂを備えている。

【０１２７】チャレンジ鍵生成回路６３１ａ，６３１ｂは、例えば乱数生成アルゴリズムを用いて、生成の都度変化するチャレンジ鍵を生成する。認証鍵生成回路６３３ａ，６３３ｂは、例えば一方向性関数を用いて、チャレンジ鍵から認証鍵を生成する。

【０１２８】比較回路６３５ａ，６３５ｂは、２つの認証鍵が一致するか否か比較する。一時鍵生成回路６３７ａ，６３７ｂは、例えば一方向性関数を利用して、２つの認証鍵から一時鍵を生成する。

【０１２９】認証鍵生成回路６３３ａと認証鍵生成回路６３３ｂは、例えば同一のアルゴリズムを用いることにより、同一のチャレンジ鍵に対して同一の認証鍵を生成するものとする。

【０１３０】一時鍵生成回路６３７ａと一時鍵生成回路６３７ｂは、例えば同一のアルゴリズムを用いることにより、同一の２つの認証鍵から同一の一時鍵を生成するものとする。

【０１３１】次に、図１５、図１６を参照しながら鍵共有の手順について説明する。まず、鍵共有手段のフェイズ１では、ノード２にて、チャレンジ鍵生成回路６３１ａによりチャレンジ鍵（ｃｈａｌｌｅｎｇｅ　Ｋｅｙ）ＣＫ１を生成し、これをノード＃１に伝える。

【０１３２】次に、ノード＃２の認証鍵生成回路６３３ａとノード＃２の認証鍵生成回路６３３ｂのそれぞれにて、チャレンジ鍵ＣＫ１をもとに認証鍵（ｋｅｙ１）Ｋ１を生成し、またノード＃１からノード＃２へ生成した認証鍵Ｋ１を転送する。

【０１３３】そしてノード＃２にて、比較回路６３５ａによりノード＃２とノード＃１のそれぞれで生成された２つの認証鍵Ｋ１を比較する。もし一致すれば次のフェイズ２に移行する。もし一致しなければ異常終了となる。

【０１３４】次に、フェイズ２では、ノード＃１にて、チャレンジ鍵生成回路６３１ｂによりチャレンジ鍵（ｃｈａｌｌｅｎｇｅ　Ｋｅｙ）ＣＫ２を生成し、これをノード＃２に伝える。

【０１３５】次に、ノード＃１の認証鍵生成回路６３３ｂとノード＃２の認証鍵生成回路６３３ａのそれぞれにて、チャレンジ鍵ＣＫ２をもとに認証鍵（ｋｅｙ２）Ｋ２を生成し、またノード＃２からノード＃１へ生成した認証鍵Ｋ２を転送する。

【０１３６】そしてノード＃１にて、比較回路６３５ｂによりノード＃１とノード＃２のそれぞれで生成された２つの認証鍵Ｋ２を比較する。もし一致すれば次のフェイズ３に移行する。もし一致しなければ異常終了となる。

【０１３７】そして、フェイズ３では、ノード＃２の一時鍵生成回路６３７ａとノード＃１の一時鍵生成回路６３７ｂのそれぞれにて、認証鍵Ｋ１と認証鍵Ｋ２をもとに一時鍵（ＢＵＳ　Ｋｅｙ）すなわち一時鍵（Ｓｋｔ）を生成する。

【０１３８】これによって、ノード＃１とノード＃２との間で安全に一時鍵Ｓｋｔが共有化される。上述したように、本発明の実施の形態に係る不正データコピー防止装置及び方法は、第１、第２又は第３の実施形態と同様な構成を設けた他、マスター鍵を用いずに送信機器と受信機器の間で一時鍵Ｓｋ を安全に共有することができるようにしたので、第１、第２又は第３の実施形態と同様な効果が得られる他、機器間を接続するケーブルから他記録媒体に記録して再利用する不正なコピーをより一層確実に防止することができる。

【０１３９】なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。また、各実施形態に記載した手法は、計算機に実行させることができるプログラムとして、例えば磁気ディスク（フロッピーディスク、ハードディスク等）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤ等）、半導体メモリ等の記憶媒体に格納し、また通信媒体により伝送して頒布することもできる。本装置を実現する計算機は、記憶媒体に記録されたプログラムを読み込み、このプログラムによって動作が制御されることにより上述した処理を実行する。

【０１４０】

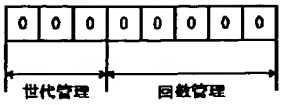
【発明の効果】以上詳記したように本発明によれば、第１の目的は、データ内のコピー管理を行う部分に対する不正者の攻撃を確実に防御できる不正データコピー防止装置及び方法並びに記録媒体を提供することができる。

【０１４１】また、本発明によれば、不正なコピーデータを有効に再生させないようにする不正データコピー防止装置及び方法を提供することができる。さらに、本発明によれば、きめ細かなコピー管理を実現できる不正データコピー防止装置及び方法を提供することができる。

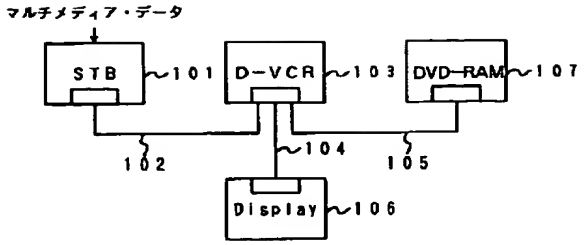
【図面の簡単な説明】

【図１】本発明の第１の実施の形態に係る不正データコピー防止装置を適用するデジタル記録再生機器の接続構成例を示すブロック図。
【図２】同実施形態に使用されるデータ構造の構成方法を説明する図。
【図３】同実施形態の不正データコピー防止装置に用いられるデータ構造例を示す図。
【図４】同実施形態の不正データコピー防止装置を用いたデジタル記録再生機器の構成例を示す図。
【図５】同実施形態のＣＦ変更部の構成及びその処理を示す図。
【図６】同実施形態のデータ再生コピー処理部の構成及びその処理を示す図。
【図７】コピー管理フラグＣＦの構成例を示す図。
【図８】コピー世代の管理ビットの状態遷移を表した図。
【図９】本発明の第２の実施形態に使用されるデータ構造の構成方法を説明する図。
【図１０】同実施形態の不正データコピー防止装置に用いられる他のデータ構造例を示す図。
【図１１】同実施形態の不正データコピー防止装置のデータ再生コピー処理部の構成及びその処理を示す図。
【図１２】本発明の第３の実施形態の不正データコピー防止装置に用いられる他のデータ構造例を示す図。
【図１３】本発明の第４の実施形態におけるマスター鍵束を利用した各機器間で一時暗号鍵を共有するための仕組みを説明した図。
【図１４】同実施形態の動作を説明する流れ図。
【図１５】本発明の第５の実施形態における鍵共有回路の構成例を示すブロック図。
【図１６】鍵共有回路によりマスター鍵束を用いずに各機器間で一時暗号鍵を共有するための仕組みを説明した図。
【符号の説明】
２１１…マスター鍵で暗号化されたコピー管理フラグＣＦとデータ暗号鍵Ｄkのペア
２１２…マスター鍵暗号化部
２１３…ディスク鍵暗号化部
２１４…データ本体
２１５…データ構造体
２２１…コピー管理フラグ部
２２２…データ暗号鍵
２２３…マスター鍵暗号化部
２２４…ディスク鍵暗号化部
２２５…データ本体
２２６…データ構造体
３０１…送信機器
３０２…受信機器
３０３…ＩＥＥＥ１３９４ケーブル
３１１，３２１，３２２…ＩＥＥＥ１３９４チップ
３１４，３３１…ＩＥＥＥ１３９４Ｉ／Ｆ部
３１５，３３２…鍵共有回路
３１６…暗号化回路
４０１…データ読み取り制御回路
４０２，４０６…メモリ
４０３，４０４，４０７，４１３…復号化回路
４０５…判定回路
４０８…ＣＦ変更回路
４０９…データ更新回路
４１０，４１６…暗号化回路
４１１…ＣＦ判定回路
４１２…鍵変更回路
４１４…ＣＦ変更回路
４１５…コピー回路
５０１…送信機器
５０２…ＩＥＥＥ１３９４ケーブル
５０３…受信機器
５０４ａ，５０４ｂ…マスター鍵束
５０５…一時鍵生成回路
５０６…一時鍵
５０７ａ，５０７ｂ…暗号化回路
５１０ａ，５１１ｂ…復号化回路
５１３…一時鍵判定回路
６３０ａ，６３０ｂ…鍵共有回路
６３１ａ，６３１ｂ…チャレンジ鍵生成回路
６３３ａ，６３３ｂ…認証鍵生成回路
６３５ａ，６３５ｂ…比較回路
６３７ａ，６３７ｂ…一時鍵生成回路
ＣＦ…コピー管理フラグ
Dk …データ暗号鍵
Mkn…マスター鍵束
Mks…各メーカに付与されたマスター鍵束
Ｓtk…一時鍵

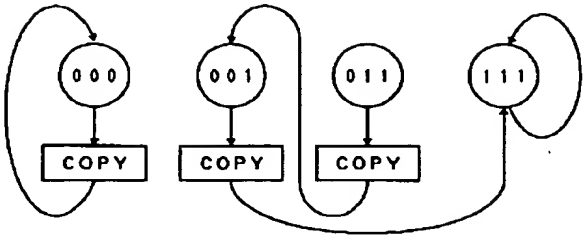
【図７】



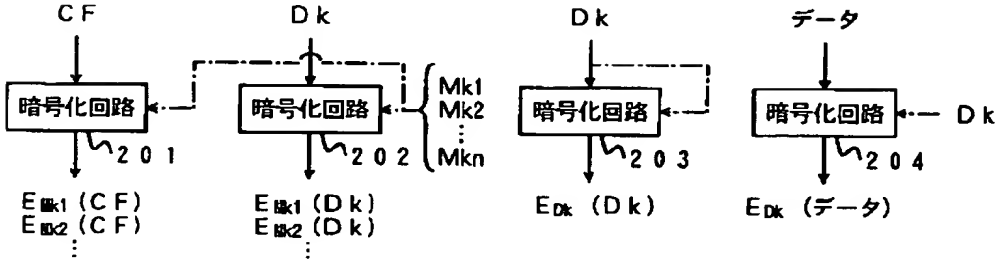
【図１】



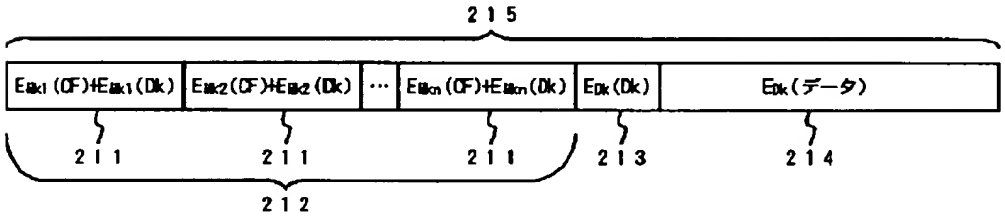
【図８】



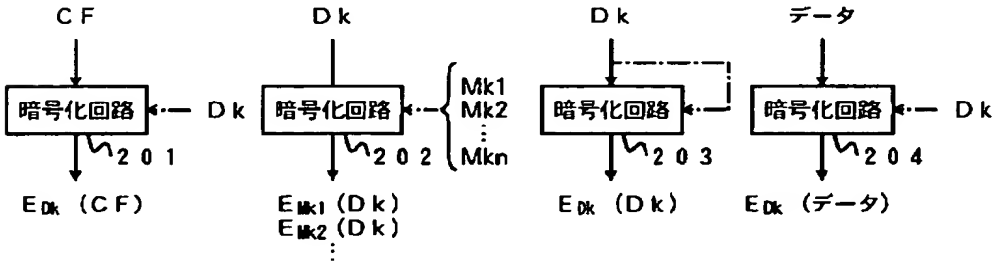
【図２】



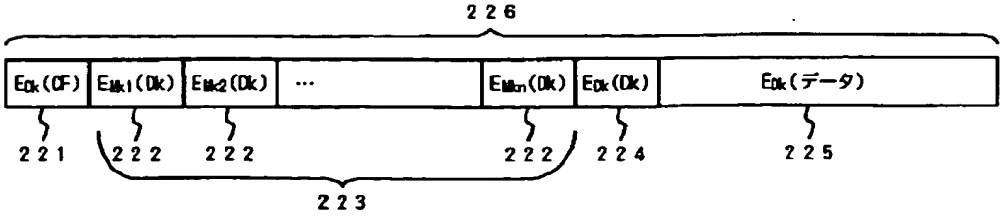
【図３】



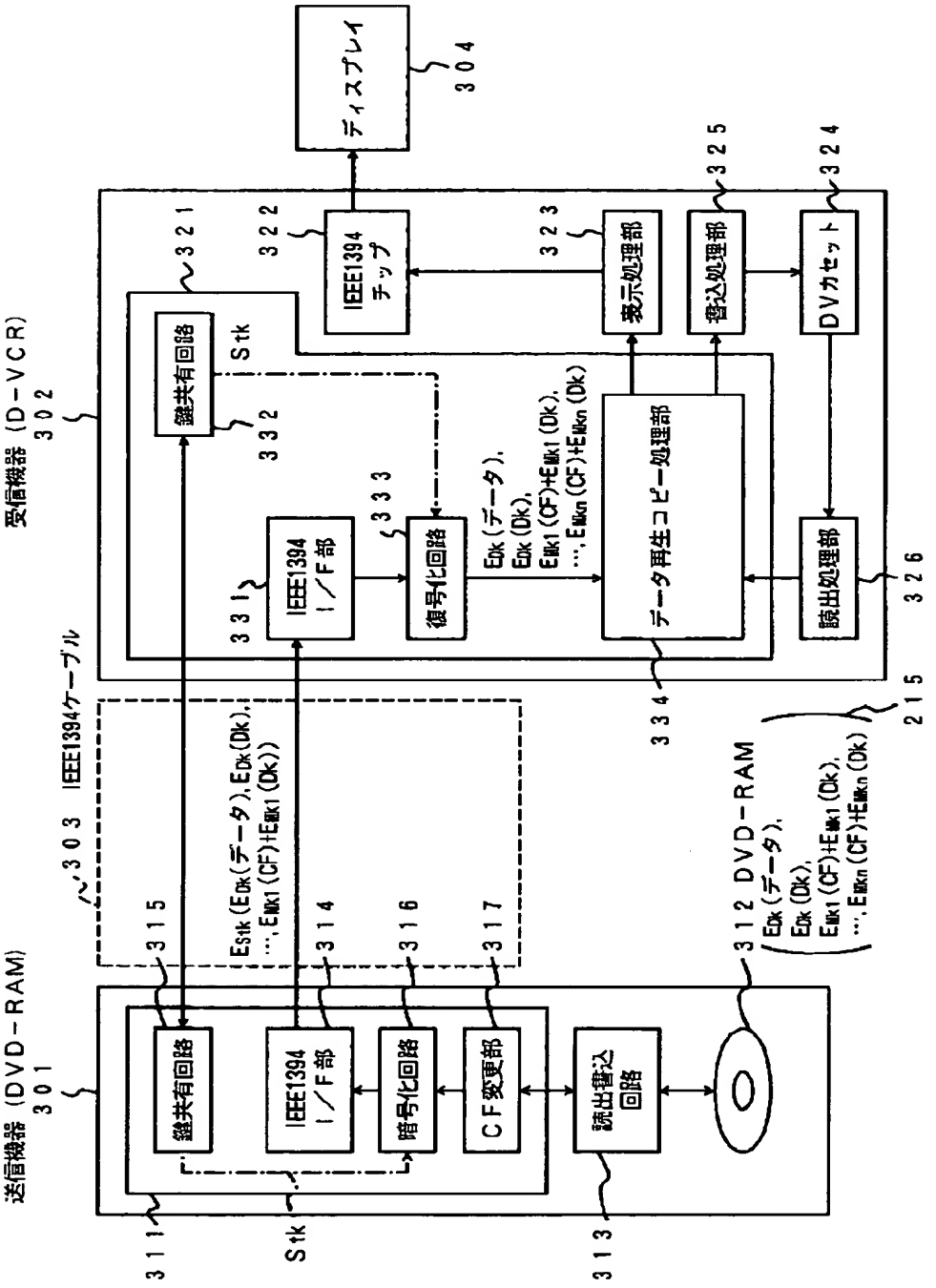
【図９】



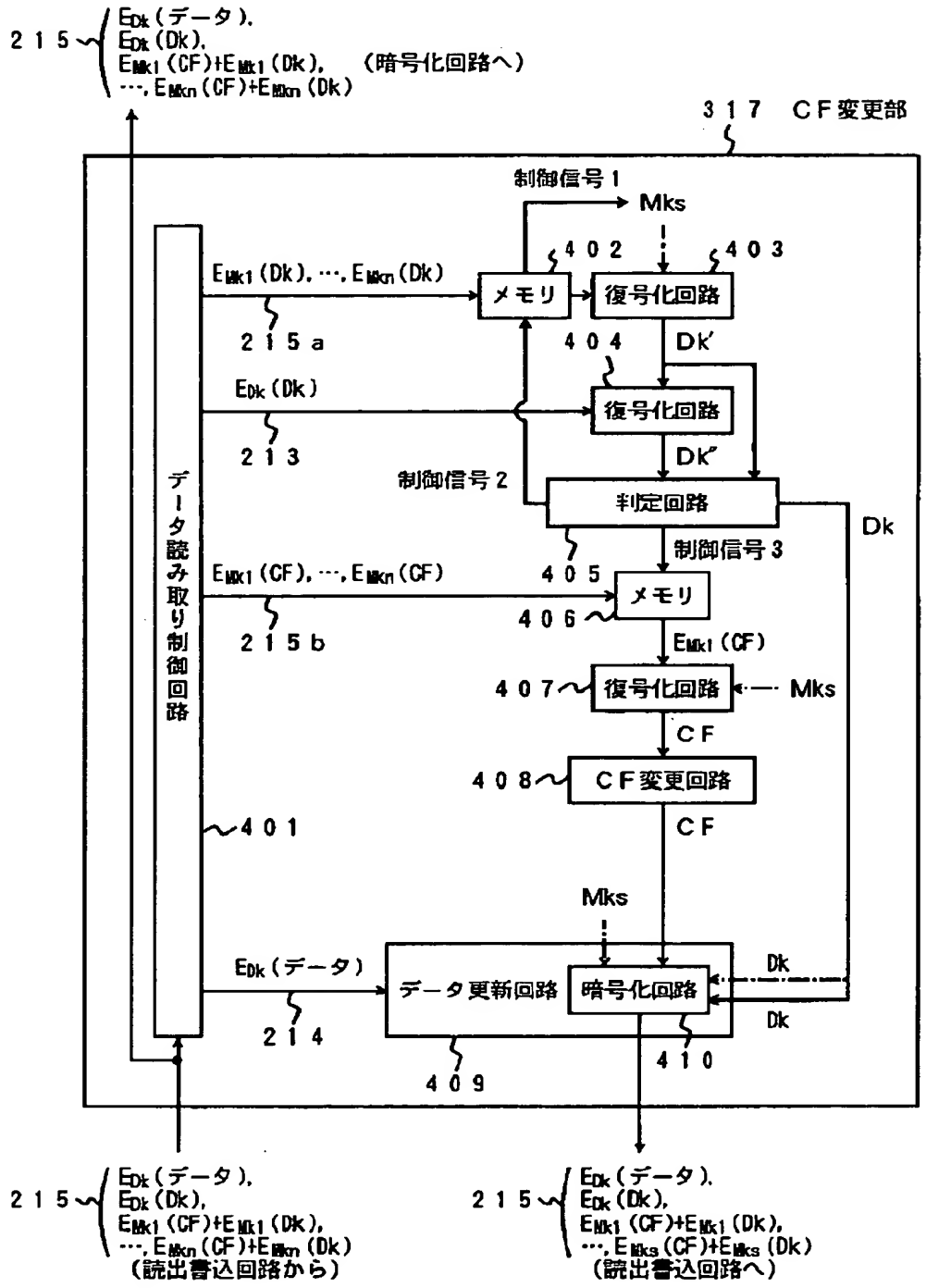
【図１０】



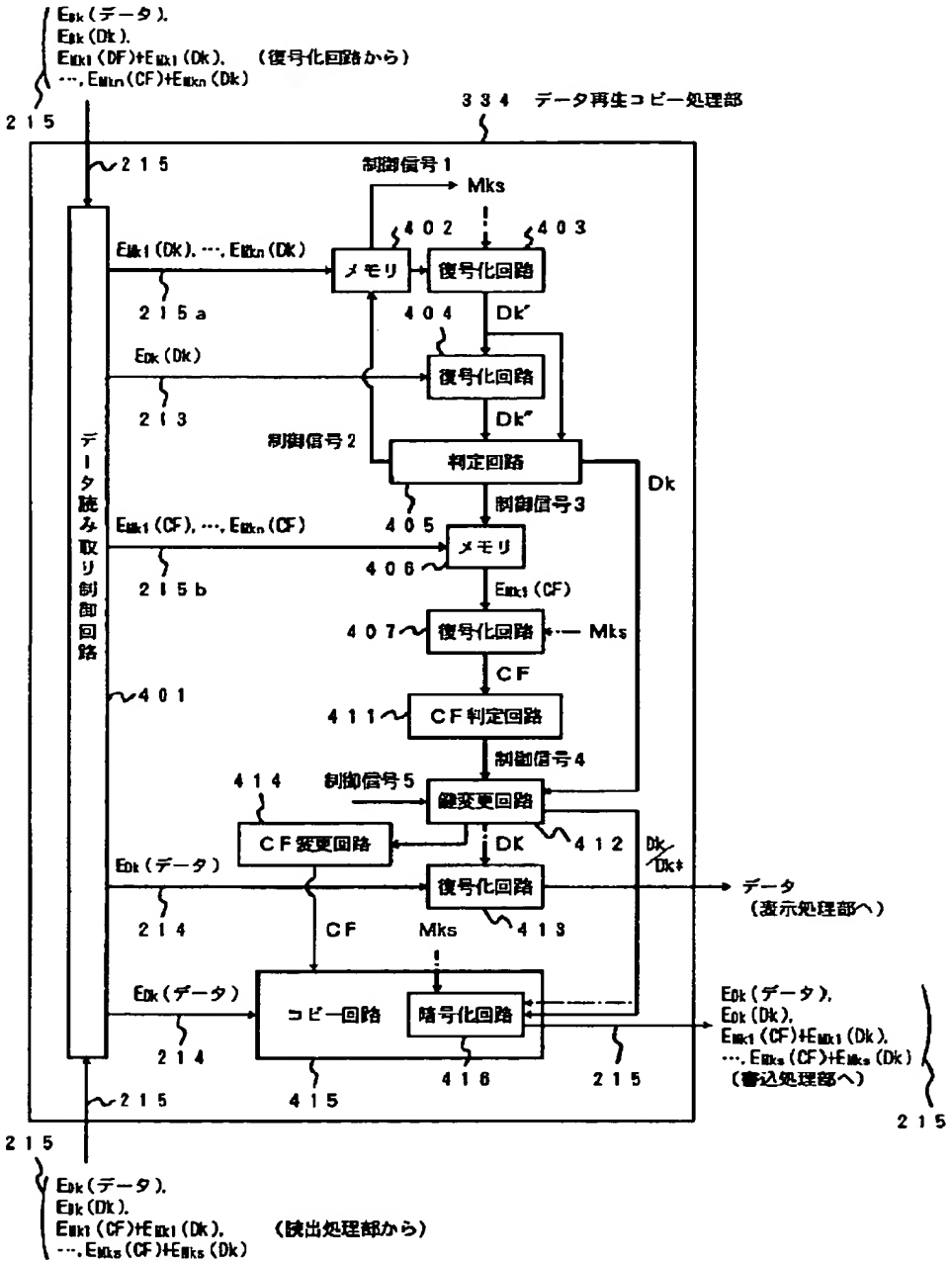
【図４】


送信機器（DVD－RAM）
301
受信機器（D－VCR）
302
IEEE1394ケーブル
303
ディスプレイ
304
鍵共有回路
311
IEEE1394 I／F部
331
暗号化回路
313
CF変更部
読出書込回路
DVD－RAM
312
IEEE1394チップ
322
表示処理部
323
書込処理部
325
DVカセット
324
復号化回路
333
データ再生コピー処理部
334
読出処理部
326
215
Stk
315
314
316
317
332
321

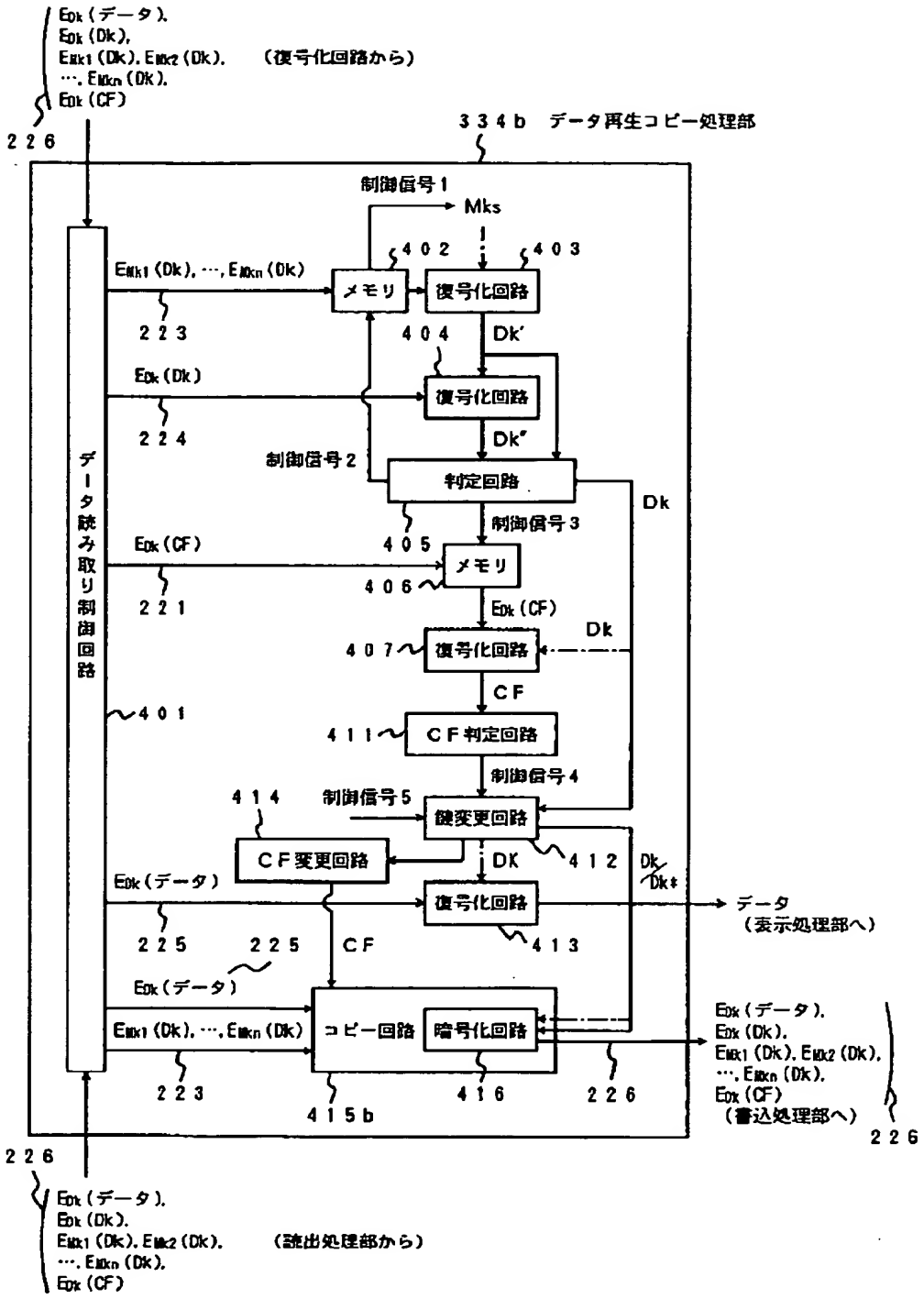
【図５】


215 EDk(データ), EDk(Dk), EMk1(CF)+EMk1(Dk), ---, EMkn(CF)+EMkn(Dk)　（暗号化回路へ）
317　CF変更部
制御信号1
Mks
402
403
EMk1(Dk), ---, EMkn(Dk)
メモリ
復号化回路
215a
404
Dk'
EDk(Dk)
復号化回路
213
Dk"
制御信号2
判定回路
Dk
制御信号3
EMk1(CF), ---, EMkn(CF)
405
メモリ
406
215b
EMk1(CF)
407
復号化回路
Mks
CF
408
CF変更回路
401
CF
データ読み取り制御回路
Mks
EDk(データ)
データ更新回路
暗号化回路
Dk
Dk
214
409
410
215 EDk(データ), EDk(Dk), EMk1(CF)+EMk1(Dk), ---, EMkn(CF)+EMkn(Dk)（読出書込回路から）
215 EDk(データ), EDk(Dk), EMk1(CF)+EMk1(Dk), ---, EMks(CF)+EMks(Dk)（読出書込回路へ）

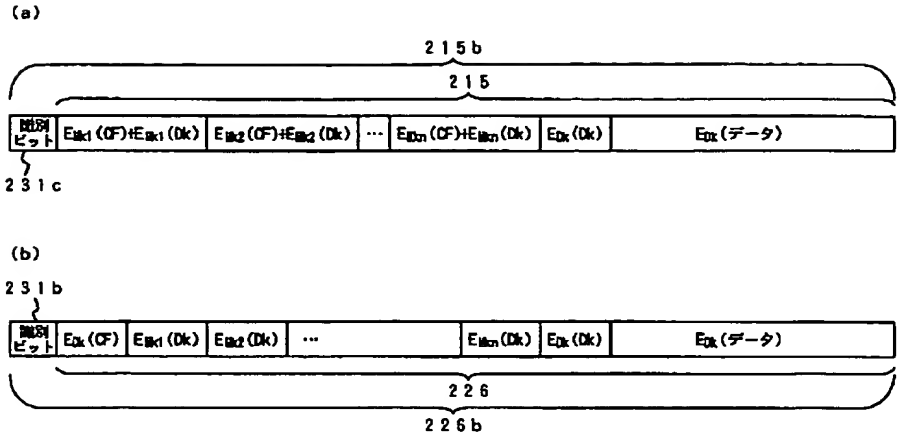
【図６】


Ebk（データ），
Edk（Dk），
Emk1（DF）+Emk1（Dk），　（復号化回路から）
…，Emkn（CF）+Emkn（Dk）
215
334　データ再生コピー処理部
215
制御信号1
Mks
402
403
Emk1（Dk），…，Emkn（Dk）
メモリ
復号化回路
215a
404
Dk'
Edk（Dk）
復号化回路
213
Dk"
制御信号2
判定回路
Dk
データ読み取り制御回路
制御信号3
Emk1（CF），…，Emkn（CF）
405
メモリ
406
215b
Emk1（CF）
407
復号化回路
Mks
CF
401
411
CF判定回路
制御信号4
414
制御信号5
鍵変更回路
CF変更回路
DK
412
Dk
Dk*
Edk（データ）
復号化回路
データ
（表示処理部へ）
214
CF
Mks
413
Edk（データ）
コピー回路
暗号化回路
Edk（データ），
Edk（Dk），
Emk1（CF）+Emk1（Dk），
…，Emks（CF）+Emks（Dk）
（書込処理部へ）
214
416
215
215
415
215
215
Edk（データ），
Edk（Dk），
Emk1（CF）+Emk1（Dk），
…，Emks（CF）+Emks（Dk），
（読出処理部から）

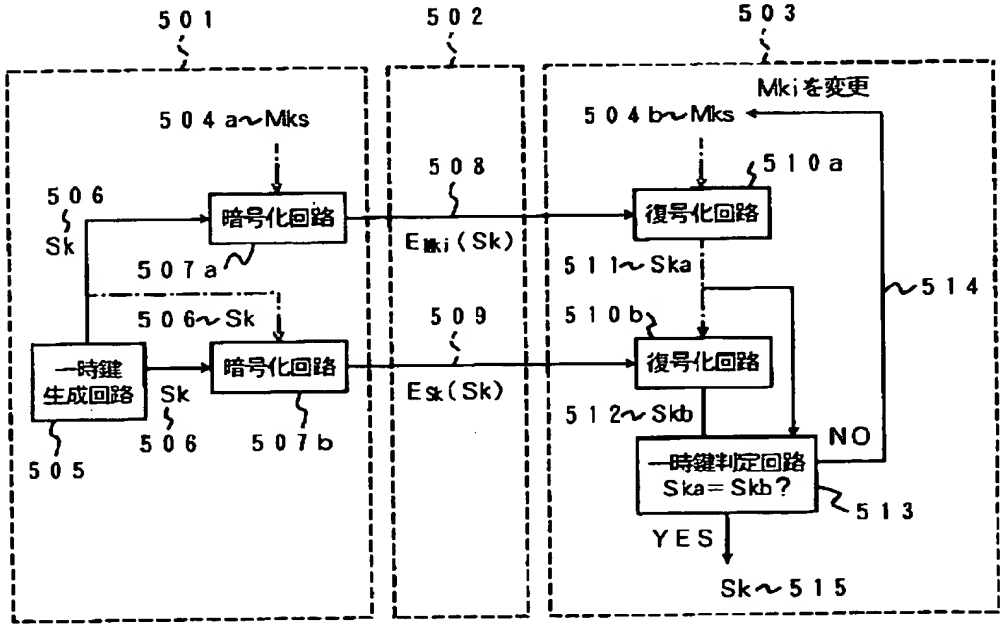
【図１１】


Edk（データ），
Edk（Dk），
Emk1（Dk），Emk2（Dk），
…，Emkn（Dk），
Edk（CF）
（復号化回路から）
226
334b　データ再生コピー処理部
制御信号1
Mks
402
403
Emk1（Dk），…，Emkn（Dk）
メモリ
復号化回路
223
404
Dk'
Edk（Dk）
復号化回路
224
Dk"
制御信号2
判定回路
Dk
制御信号3
データ読み取り制御回路
Edk（CF）
405
メモリ
406
221
Edk（CF）
Dk
407
復号化回路
CF
401
411
CF判定回路
制御信号4
414
制御信号5
鍵変更回路
CF変更回路
DK
412
Dk
Dk*
Edk（データ）
復号化回路
データ
（表示処理部へ）
225
225
CF
413
Edk（データ）
Emk1（Dk），…，Emkn（Dk）
コピー回路
暗号化回路
Edk（データ），
Edk（Dk），
Emk1（Dk），Emk2（Dk），
…，Emkn（Dk），
Edk（CF）
（書込処理部へ）
223
415b
416
226
226
226
Edk（データ），
Edk（Dk），
Emk1（Dk），Emk2（Dk），
…，Emkn（Dk），
Edk（CF）
（読出処理部から）

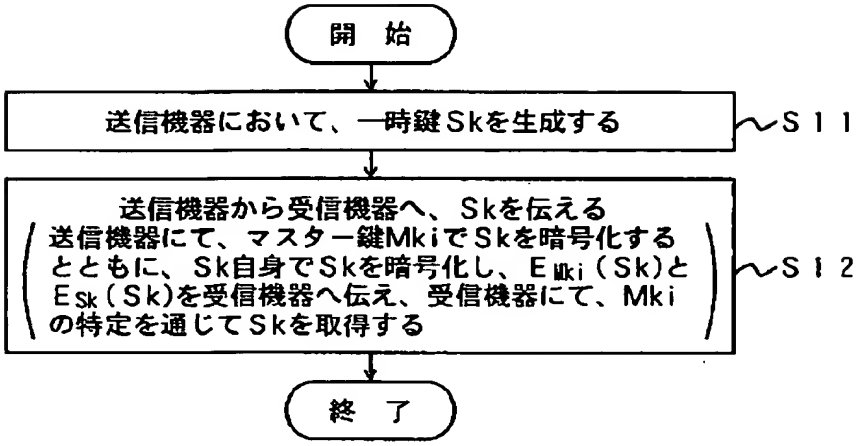
【図１２】


(a)
215b
215
識別ビット
Eak1(CF)+Eak1(Dk)
Eak2(CF)+Eak2(Dk)
…
Eakn(CF)+Eakn(Dk)
Edk(Dk)
Edk(データ)
231c
(b)
231b
識別ビット
Edk(CF)
Eak1(Dk)
Eak2(Dk)
…
Eakn(Dk)
Edk(Dk)
Edk(データ)
226
226b

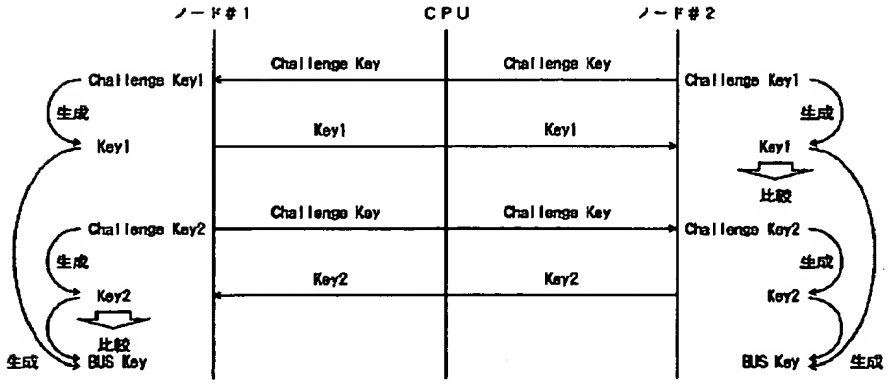
【図１３】


501
502
503
504a～Mks
504b～Mks
Mkiを変更
506
Sk
暗号化回路
507a
506～Sk
一時鍵生成回路
Sk
506
505
暗号化回路
507b
508
Eaki(Sk)
509
Esk(Sk)
510a
復号化回路
511～Ska
510b
復号化回路
512～Skb
一時鍵判定回路
Ska=Skb?
NO
514
513
YES
Sk～515

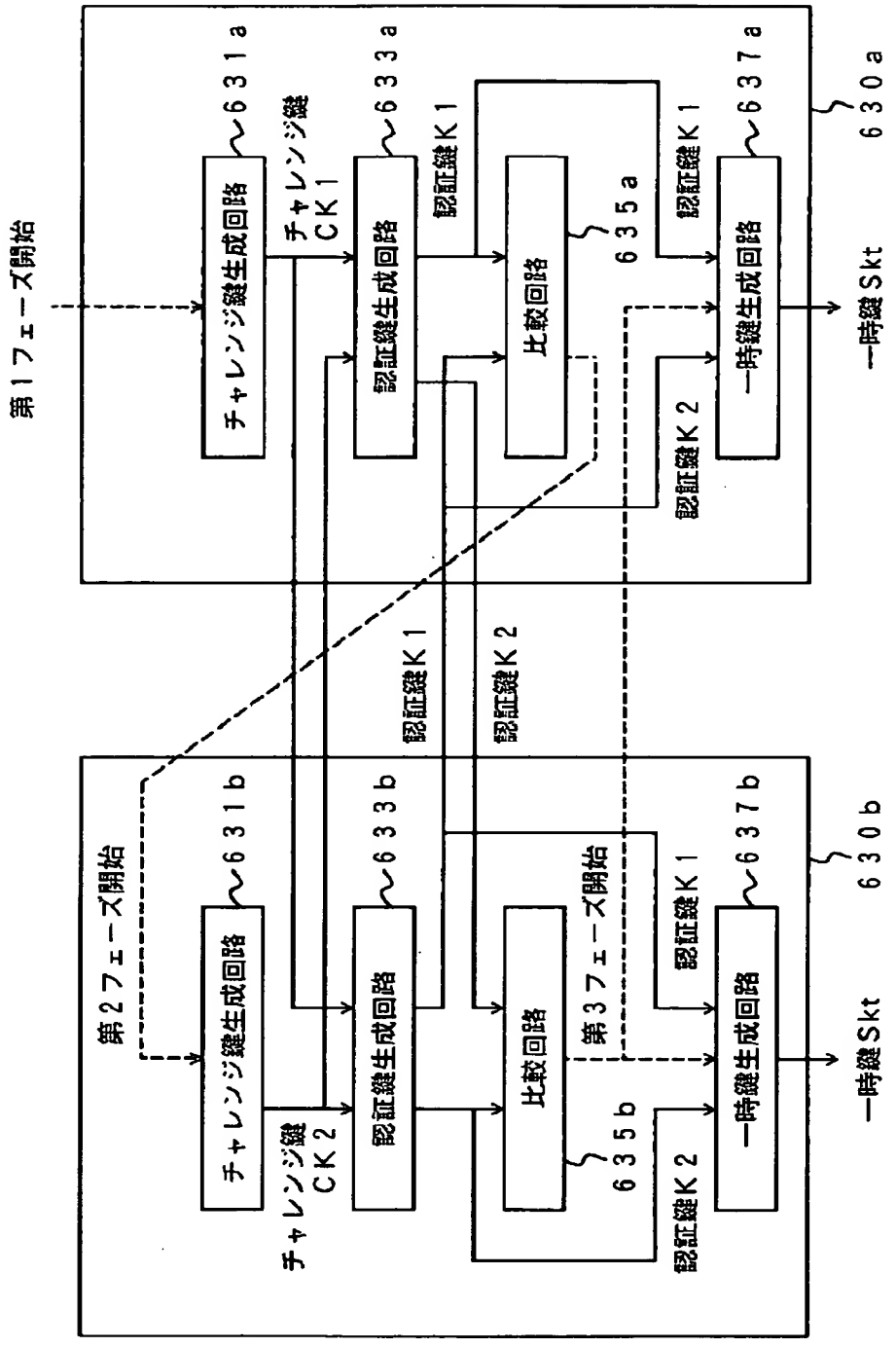
【図１４】


開　始
送信機器において、一時鍵Skを生成する
S１１
送信機器から受信機器へ、Skを伝える
送信機器にて、マスター鍵MkiでSkを暗号化するとともに、Sk自身でSkを暗号化し、E_{Mki}(Sk)とE_{Sk}(Sk)を受信機器へ伝え、受信機器にて、Mkiの特定を通じてSkを取得する
S１２
終　了

【図１６】


ノード#1
CPU
ノード#2
Challenge Key
Challenge Key
Challenge Key1
生成
Key1
Key1
Key1
生成
比較
Challenge Key
Challenge Key
Challenge Key2
Challenge Key2
生成
Key2
Key2
Key2
生成
比較
生成
BUS Key
BUS Key
生成

【図１５】



フロントページの続き

(51) Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｌ　9/36		Ｈ０４Ｌ　9/00	６８５